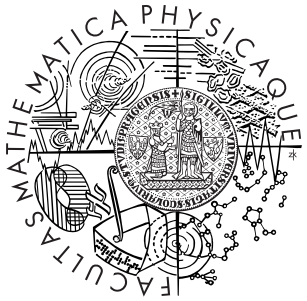
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Jakub Bulín

Vybrané partie z teorie krotkých kongruencí
(Selected Topics from Tame Congruence Theory)

Katedra algebry

Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
Studijní program: Matematika, obecná matematika

2008

Děkuji Mgr. Liboru Bartovi, Ph.D. za hodnotné rady a odborné vedení během psaní této práce.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne 29. května 2008 Jakub Bulín

Contents

Název práce: Vybrané partie z teorie krotkých kongruencí
Autor: Jakub Bulín
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Libor Barto, Ph.D.
e-mail vedoucího: libor.barto@gmail.com

Abstrakt: V předložené práci studujeme teorii krotkých kongruencí, hlubokou strukturní teorii konečných algeber. Tato teorie se ukázala být překvapivě užitečnou a od svého vzniku na počátku osmdesátých let 20. století nachází stále více aplikací jak v univerzální algebře, tak i v jiných matematických oborech, jako například v teoretické informatice. Předložená práce popisuje základy teorie krotkých kongruencí, vyložené v několika prvních kapitolách knihy The Structure of Finite Algebras od D. Hobbyho a R. McKenzieho [3]. Práce dále obsahuje řešená cvičení z výše uvedené knihy.

Klíčová slova: teorie krotkých kongruencí, univerzální algebra

Title: Selected Topics from Tame Congruence Theory
Author: Jakub Bulín
Department: Department of Algebra
Supervisor: Mgr. Libor Barto, Ph.D.
Supervisor's e-mail address: libor.barto@gmail.com

Abstract: In the present work we study the tame congruence theory; a deep structural theory of finite algebras. This theory has turned out to be surprisingly useful and since its discovery in the early eighties of the 20th century it is finding increasingly many applications in universal algebra and other fields of mathematics, as for example theoretical informatics. The present work describes the basics of tame congruence theory which are covered in a first few chapters of the book The Structure of Finite Algebras by D. Hobby and R. McKenzie [3]. Furthermore, the work contains solved excercises from the above-mentioned book.

Keywords: tame congruence theory, universal algebra

Chapter 0

Introduction

Tame congruence theory is a deep structural theory of finite algebras with surprisingly many applications in universal algebra and other fields of mathematics, as for example theoretical informatics. It is of very recent origin, the most crucial results for the theory were obtained in the early 1980's.

It is well known since the origins of universal algebra that many properties of an algebra are connected with the properties of its lattice of congruences. The idea to study this connection is essential for tame congruence theory.

Given a finite algebra, the prime quotients of its congruence lattice are divided into five types. Each type is associated with a particular kind of algebra. The properties of these algebras carry over to some extent to the corresponding type. The five types are the following: **1** – a finite set with a group of permutations, **2** – a vector space over a finite field, **3** – the two-element Boolean algebra, **4** – the two-element lattice, **5** – the two-element semilattice.

In the book [3], not only prime quotients of the congruence lattice are typed. Tame congruence theory is introduced there in a slightly more general setting. Instead of prime quotients, the so-called "tame" quotients are typed. However, in many applications it is sufficient to investigate the types of prime quotient. Therefore, in the present work we abandoned this generalization which allowed us to simplify some of the proofs from [3].

The first chapter of this work introduces some basics of universal algebra and notions that are needed later. The second chapter contains basics of tame congruence theory while in the third chapter we discover the five abovementioned types. Throughout all three chapter there are solved excercises

from the book [3].

Let us now mention some of the most important applications of tame congruence theory. In chapter 8 of the book [3], locally finite congruence modular and congruence distributive varieties are characterized in terms of ommitting some of the types mentioned above. Some deep results about decidability of certain first order theories were proved using tame congruence theory, namely in [4] and [5].

Tame cogruence theory has also proved to be very useful in theoretical informatics. In particular, it has surprising applications in the computational complexity and the constraint satisfaction problem. Let us mention here the work of Bulatov, Krokhin and Jeavons [1].

There are more applications of tame cogruence theory. It was succesfully used to study the natural dualities (see [2]) or for example the free spectra (first results are in [3], chapter 12).

Chapter 1

Preliminaries

1.1 Algebras, clones

By an *algebra* we mean a structure $\mathbf{A} = \langle A, F \rangle$, where A is a nonvoid set (the *universe* of $\mathbf{A}$) and F, the set of *basic operations* of $\mathbf{A}$, is a set of finitary operations on A (i.e., for each $f \in F$ there exists $n \geq 0$ such that $f : A^n \to A$).

The *projections* on the set A are the operations $p_n^i \, (n \in \mathbb{N}, 0 \leq i < n)$ satisfying $p_n^i(x_0, x_1, \ldots, x_{n-1}) = x_i$. A set of operations on A is called a *clone* iff it is closed under composition of operations and contains all projections. The *clone of term operations* of $\mathbf{A}$, denoted $\operatorname{Clo} \mathbf{A}$, is the clone generated by the basic operations. By $\operatorname{Clo}_n \mathbf{A}$ we mean the set of n-ary operations from $\operatorname{Clo} \mathbf{A}$.

The *clone of polynomial operations* of $\mathbf{A}$, denoted $\operatorname{Pol} \mathbf{A}$, is the clone generated by the basic operations together with all constant operations on A. By $\operatorname{Pol}_n \mathbf{A}$ we mean the set of n-ary operations from $\operatorname{Pol} \mathbf{A}$. We will be especially interested in $\operatorname{Pol}_1 \mathbf{A}$, the set of so-called *unary polynomials* of $\mathbf{A}$. Notice that $\langle \operatorname{Pol}_1 \mathbf{A}, \circ, \mathrm{id}_A \rangle$ is a monoid (i.e., semigroup with identity element id_A; here "$\circ$" denotes composition of functions).

We can also regard $\operatorname{Clo}_n \mathbf{A}$ as the subuniverse of the direct power $\mathbf{A}^{A^n}$ generated by n-ary projections. Similarly, $\operatorname{Pol}_n \mathbf{A}$ is the subuniverse of $\mathbf{A}^{A^n}$ generated by the n-ary projections together with all the constant n-ary operations.

Let $U \subseteq A$ be any subset. Let $f : A^n \to A$ be a function for some $n \geq 0$.

The *restriction of f to U* is defined as

$$f|_U \stackrel{\text{def}}{=} \{\langle x_0, x_1, \ldots, x_{n-1}, f(x)\rangle \,:\, x_i \in U \text{ for } 0 \leq i < n\}.$$

We say that U is *closed under* f iff $f(U^n) \subseteq U$. If f is an operation on A and U is closed under f, then the restriction $f|_U$ is obviously an operation on U. We define

$$(\operatorname{Pol}\mathbf{A})|_U \stackrel{\text{def}}{=} \{f|_U \,:\, f \in \operatorname{Pol}\mathbf{A}, U \text{ is closed under } f\}.$$

1.1 Definition. Let $\mathbf{A}$ be any algebra and U a nonvoid subset of its universe. We define the **algebra induced on U by $\mathbf{A}$** (or the **induced algebra** if $\mathbf{A}$ and U are known from the context) to be the algebra

$$\mathbf{A}|_U \stackrel{\text{def}}{=} \langle U, (\operatorname{Pol}\mathbf{A})|_U\rangle.$$

1.2 Excercise. For any algebra $\mathbf{A}$ and $\emptyset \neq U \subseteq A$,

$$(\operatorname{Pol}\mathbf{A})|_U = \operatorname{Clo}(\mathbf{A}|_U) = \operatorname{Pol}(\mathbf{A}|_U),$$

i.e., every polynomial operation of $\mathbf{A}|_U$ is already its basic operation.

Proof. The basic operations of $\mathbf{A}|_U$ are precisely $(\operatorname{Pol}\mathbf{A})|_U$, so trivially

$$(\operatorname{Pol}\mathbf{A})|_U \subseteq \operatorname{Pol}(\mathbf{A}|_U).$$

Now, notice that $(\operatorname{Pol}\mathbf{A})|_U$ is a clone (it is closed under composition and contains all projections). Moreover, it contains all constant operations and, of course, the basic operations of $\mathbf{A}|_U$. Therefore

$$\operatorname{Pol}(\mathbf{A}|_U) \subseteq (\operatorname{Pol}\mathbf{A})|_U$$

from the definition of the clone of polynomial operations. The rest is obvious. □

1.3 Definition. An **idempotent** in $\operatorname{Pol}_1\mathbf{A}$ is such $e \in \operatorname{Pol}_1\mathbf{A}$ that $e = e^2 (= e \circ e)$. The set of all idempotents in $\operatorname{Pol}_1\mathbf{A}$ will be denoted by $\operatorname{E}(\mathbf{A})$.

Notice that for any $e \in \operatorname{E}(\mathbf{A})$, the restriction of e to its range is the identity, i.e. if $U = e(A)$, then $e|_U = \operatorname{id}_U$.

1.4 Excercise. Let $\mathbf{A}$ be an algebra. If $e \in \mathrm{E}(\mathbf{A})$ and $\emptyset \neq N \subseteq U = e(A)$, then

$$\mathbf{A}|_N = (\mathbf{A}|_U)|_N.$$

Proof. Both algebras have the same universe N. We want to prove that $(\operatorname{Pol}\mathbf{A})|_N = (\operatorname{Pol}\mathbf{A}|_U)|_N$. Let $f \in \operatorname{Pol}\mathbf{A}$ be such that N is closed under f. We have that U is closed under ef and from $e|_U = \mathrm{id}_U$ and $N \subseteq U$ it follows that $ef|_N = f|_N$, therefore $f|_N \in (\mathbf{A}|_U)|_N$. The other inclusion follows immediately from the fact that $(f|_U)|_N = f|_N$. □

1.5 Lemma. *Let* $\mathbf{A}$ *be a finite algebra. There exists* $n > 0$ *such that for all* $f \in \operatorname{Pol}_1\mathbf{A}$*,* f^n *is idempotent (i.e.,* $f^n = f^{2n}$*).*

Proof. Fix $x \in \mathbf{A}$ and $f \in \operatorname{Pol}_1\mathbf{A}$. The set $\{f(x), f^2(x), f^3(x), \dots\}$ is finite, so there must exist $k, l \in \mathbb{N}$ such that $f^k(x) = f^l(x)$. We can demand $k < l \leq |A|$. Denote by p the period $l - k$. We have that $f^j = f^{j+p}$ for all $j \geq k$.

We define $n = |A|!$. Now, $n \geq k$ and p divides n. Therefore

$$f^{2n}(x) = f^{n+n}(x) = f^{n+\frac{n}{p}p} = f^n(x).$$

The definition of n is independent of the choice of x and f, thus the statement is proved. □

Note that the statement of the previous lemma holds for the set of all mappings $f : A \to A$ instead of $\operatorname{Pol}_1\mathbf{A}$. It can also be easily generalized for any finite semigroup.

1.2 Congruences

Recall that an *equivalence* is a reflexive, symmetric and transitive relation. The set of all equivalences on A, ordered by inclusion, forms a complete algebraic lattice, we denote it Π_A. Let $\theta \in \Pi_A$ and $x \in A$. We put $x/\theta = \{y : \langle x, y\rangle \in \theta\}$. The set $A/\theta = \{x/\theta : x \in A\}$ is a *partition* of $\mathbf{A}$. The elements of A/θ are called *(equivalence) classes* of θ, or *θ-classes*. The least element of Π_A is $0_A = \{\langle x, x\rangle : x \in A\}$ and the largest is $1_A = A^2$.

Let f be an operation on A (say f is n-ary) and $\theta \in \Pi_A$. We say that f *preserves* θ iff $\langle f(x), f(y)\rangle \in \theta$ for all $\langle x, y\rangle \in \theta$. A *congruence* of $\mathbf{A}$ is an equivalence on A preserved by all the basic operations of $\mathbf{A}$. Note that $\theta \in \Pi_A$ is a congruence of $\mathbf{A}$ iff it is a subuniverse of $\mathbf{A}^2$.

The set of all congruences of $\mathbf{A}$, ordered by inclusion, forms a complete algebraic lattice, the *lattice of congruences of* $\mathbf{A}$, denoted $\operatorname{Con}\mathbf{A}$. The meet of two congruences in $\operatorname{Con}\mathbf{A}$ is simply their intersection while the join is the transitive closure of their union.

It is easy to show that the algebras $\mathbf{A}$, $\langle A, \operatorname{Clo}\mathbf{A}\rangle$, $\langle A, \operatorname{Pol}\mathbf{A}\rangle$, $\langle A, \operatorname{Pol}_1\mathbf{A}\rangle$ have the same lattices of congruences (i.e., $\theta \in \Pi_A$ is a congruence of one of them iff it is a congruence of all of them).

Let f be an arbitrary mapping with domain A and $\theta \in \Pi_A$. By $f(\theta)$ we mean the set $\{\langle f(x), f(y)\rangle : \langle x, y\rangle \in \theta\}$. If $f \in \operatorname{Pol}_1\mathbf{A}$ and $\alpha \in \operatorname{Con}\mathbf{A}$, then $f(\alpha) \subseteq \alpha$.

Let $U \subseteq A$ be any subset and $\theta \in \Pi_A$. The *restriction of* θ *to* U is defined as

$$\theta|_U \stackrel{\text{def}}{=} \theta \cap (U \times U).$$

It is easily seen that $\theta|_U \in \operatorname{Con}\mathbf{A}|_U$.

Let $\langle S, \circ\rangle$ be a semigroup (e.g., $\operatorname{Pol}_1\mathbf{A}$) and $K, L \subseteq S$ its nonvoid subsets. By KL we mean the set $\{f \circ g : f \in K, g \in L\}$. K is a *right ideal* in $\langle S, \circ\rangle$ iff $KS = K$.

1.6 Excercise. Let $\mathbf{A}$ be any algebra and K a right ideal in $\operatorname{Pol}_1\mathbf{A}$. Define a mapping μ_K of $\operatorname{Con}\mathbf{A}$ by

$$\mu_K(\theta) = \{\langle x, y\rangle \in \mathbf{A}^2 : \langle g(x), g(y)\rangle \in \theta \text{ for all } g \in K\}.$$

The following statements hold.

(i) $\mu_K(\theta) \in \operatorname{Con}\mathbf{A}$, $\theta \subseteq \mu_K(\theta)$ for all $\theta \in \operatorname{Con}\mathbf{A}$; μ_K is a meet endomorphism of $\operatorname{Con}\mathbf{A}$ (i.e., $\mu_K(\alpha \wedge \beta) = \mu_K(\alpha) \wedge \mu_K(\beta)$ for all $\alpha, \beta \in \operatorname{Con}\mathbf{A}$).

(ii) For right ideals K, L in $\operatorname{Pol}_1\mathbf{A}$ and $\theta \in \operatorname{Con}\mathbf{A}$,

  (a) $\mu_K(\theta) = \mu_{(\operatorname{Pol}_1\mathbf{A})K}(\theta)$,

  (b) $\mu_{KL}(\theta) = \mu_L\mu_K(\theta)$,

  (c) $\mu_{KL}(\theta) \supseteq \mu_K(\theta) \vee \mu_L(\theta)$.

Proof. Obviously, $\mu_K(\theta)$ is an equivalence. Choose arbitrary $f \in \operatorname{Pol}_1\mathbf{A}$. Since K is a right ideal, we have that $gf \in K$ for all $g \in K$. Therefore $\langle f(x), f(y)\rangle \in \mu_K(\theta)$ for all $\langle x, y\rangle \in \mu_K(\theta)$. This proves $\mu_K(\theta) \in \operatorname{Con}\mathbf{A}$. If $\langle x, y\rangle \in \theta$, then $\langle g(x), g(y)\rangle \in \theta$ for all $g \in \operatorname{Pol}_1\mathbf{A} \supseteq K$, therefore $\theta \subseteq \mu_K(\theta)$. The meet of two congruences in $\operatorname{Con}\mathbf{A}$ is their intersection. From this fact it follows immediately that μ_K is a meet endomorphism.

Let us prove (a). The first inclusion is obvious, since $\langle g(x), g(y)\rangle \in \theta$ implies that $\langle fg(x), fg(y)\rangle \in \theta$ for all $f \in \mathrm{Pol}_1 \mathbf{A}$. Now, if we have $\langle fg(x), fg(y)\rangle \in \theta$ for all $f \in \mathrm{Pol}_1 \mathbf{A}$ and $g \in K$, we also have that $\langle g(x), g(y)\rangle = \langle \mathrm{id}_A\, g(x), \mathrm{id}_A\, g(y)\rangle \in \theta$, and the other inclusion is proved.

Now, (b) follows from the fact that $\langle gh(x), gh(y)\rangle \in \theta$ for all $g \in K, h \in L$ iff $\langle h(x), h(y)\rangle \in \mu_K(\theta)$ for all $h \in L$.

Finally, let us prove (c). From (i) we see that $\mu_K(\theta) \subseteq \mu_L\mu_K(\theta)$. Since $\theta \subseteq \mu_K(\theta)$, it is also easily seen that $\mu_L(\theta) \subseteq \mu_L\mu_K(\theta)$. By (b), $\mu_L\mu_K(\theta) = \mu_{KL}(\theta)$. We conclude that the join $\mu_K(\theta) \vee \mu_L(\theta)$ is also contained in $\mu_{KL}(\theta)$. □

1.3 Quotient algebras

Let f be an operation on A (say f is n-ary) and let $\theta \in \Pi_A$ be preserved by f. We define the n-ary operation f_θ on A/θ in the following way:

$$f_\theta(x_0/\theta, x_1/\theta, \ldots, x_{n-1}/\theta) \stackrel{\mathrm{def}}{=} f(x_0, x_1, \ldots, x_{n-1})/\theta.$$

Let $\alpha \in \mathrm{Con}\,\mathbf{A}$. We define the *quotient algebra of* $\mathbf{A}$ *over* α as the algebra $\langle A/\alpha, f_\alpha\,(f \in F)\rangle$ of the same type as $\mathbf{A}$. Notice that the congruences of $\mathbf{A}$ are precisely the kernels of homomorphisms from $\mathbf{A}$.

1.7 Lemma. *Let* $\mathbf{A}$ *be any algebra and* $\alpha \in \mathrm{Con}\,\mathbf{A}$. *Then*

$$\mathrm{Pol}\,\mathbf{A}/\alpha = \{f_\alpha \,:\, f \in \mathrm{Pol}\,\mathbf{A}\}.$$

Moreover, $\mathrm{Pol}_n\,\mathbf{A}/\alpha = \{f_\alpha \,:\, f \in \mathrm{Pol}_n\,\mathbf{A}\}$ *for all* $n > 0$.

Proof. All $f \in \mathrm{Pol}\,\mathbf{A}$ preserve α, so the definition is correct. Let us denote $\{f_\alpha \,:\, f \in \mathrm{Pol}\,\mathbf{A}\}$ by K. It is easily seen that K contains all projections, constant operations and that it is closed under composition, therefore $\mathrm{Pol}\,\mathbf{A}/\alpha \subseteq K$.

On the other hand, if $f \in \mathrm{Pol}\,\mathbf{A}$ is a basic operation, projection or constant, then $f/\alpha \in \mathrm{Pol}\,\mathbf{A}/\alpha$. Moreover, if h is a composition of $f, g \in \mathrm{Pol}\,\mathbf{A}$, then h/α is a composition of $f/\alpha, g/\alpha$, which finishes the proof, since the rest is obvious. □

Chapter 2

Minimal sets

In this chapter, all the algebras considered will be assumed to be finite. We will now introduce the key notion of the $\langle \alpha, \beta \rangle$-*minimal set*.

2.1 Basic notions

2.1 Definition. Let $\mathbf{A}$ be a finite algebra and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, $\alpha \prec \beta$. We define

$$\mathrm{U}_{\mathbf{A}}(\alpha, \beta) = \{f(A) : f \in \operatorname{Pol}_1 \mathbf{A} \text{ and } f(\beta) \not\subseteq \alpha\}.$$

We define $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ to be the set of all minimal members of $\mathrm{U}_{\mathbf{A}}(\alpha, \beta)$ (with respect to inclusion). Members of $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ are called $\langle \alpha, \beta \rangle$-**minimal sets** of $\mathbf{A}$.

The following observation is an immediate consequence of the definition of $\langle \alpha, \beta \rangle$-minimality:

2.2 Observation. *Let $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $U = f(A)$ for some $f \in \operatorname{Pol}_1 \mathbf{A}$ such that $f(\beta) \not\subseteq \alpha$. Then for each $g \in \operatorname{Pol}_1 \mathbf{A}$, either $fg(\beta) \subseteq \alpha$ or $fg(A) = U$.*

Proof. Since $g(A) \subseteq A$, it follows that $fg(A) \subseteq f(A) = U$. Thus by the $\langle \alpha, \beta \rangle$-minimality of U, if $fg(\beta) \not\subseteq \alpha$ then $fg(A) = U$. □

2.3 Theorem. *Let $\mathbf{A}$ be a finite algebra and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, $\alpha \prec \beta$. We define*

$$\mathrm{N}_{\mathbf{A}}(\alpha, \beta) = \{e(A) : e \in \mathrm{E}(\mathbf{A}) \text{ and } e(\beta) \not\subseteq \alpha\}.$$

Each $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ is a member of $\mathrm{N}_{\mathbf{A}}(\alpha, \beta)$. Moreover, the $\langle \alpha, \beta \rangle$-minimal sets of $\mathbf{A}$ are precisely the minimal members of $\mathrm{N}_{\mathbf{A}}(\alpha, \beta)$ (with respect to inclusion).

Proof. Choose $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. We want to prove that there exists $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) = U$ and $e(\beta) \not\subseteq \alpha$.

Denote $K = \{g \in \mathrm{Pol}_1 \mathbf{A} : g(A) \subseteq U\}$. K is a right ideal in the monoid $\mathrm{Pol}_1 \mathbf{A}$ (i.e., $gh \in K$ for any $g \in K$ and $h \in \mathrm{Pol}_1 \mathbf{A}$). Consider the relation

$$\theta = \{\langle x, y\rangle \in \beta : \langle g(x), g(y)\rangle \in \alpha \text{ for all } g \in K\}.$$

If we adopt the notation from Excercise 1.6, we see that $\theta = \mu_K(\alpha) \wedge \beta$. It follows that $\theta \in \mathrm{Con}\,\mathbf{A}$ and $\alpha \leq \theta \leq \beta$.

From the definition of $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ we have $U = f(A)$ for some $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\beta) \not\subseteq \alpha$. We have that $f \in K$ and there exists $\langle a, b\rangle \in \beta$ such that $\langle f(a), f(b)\rangle \notin \alpha$, which implies $\theta < \beta$. We conclude that $\theta = \alpha$.

Since $\langle f(a), f(b)\rangle \notin \alpha = \theta$, there exists $g \in K$ such that $\langle gf(a), gf(b)\rangle \notin \alpha$. We have that $gf(A) \subseteq U$ and $gf(\beta) \not\subseteq \alpha$, thus by the $\langle \alpha, \beta\rangle$-minimality of U we get

$$gf(A) = g(U) = U.$$

We now define $e = g^k$ with $k > 0$ such that $g^k = g^{2k}$ (see Lemma 1.5). We have $e \in \mathrm{E}(\mathbf{A})$ and $U = e(U) \subseteq e(A)$ which together with $e \in K$ implies $U = e(A)$.

Now we will prove that $e(\beta) \not\subseteq \alpha$. Since $e|_U = \mathrm{id}_U$, we have that

$$e(\beta) \subseteq \beta|_U = e(\beta|_U) \subseteq e(\beta),$$

and so $e(\beta) = \beta|_U$. But from $f(\beta) \not\subseteq \alpha$ and $f(\beta) \subseteq \beta|_U$ we get that $\beta|_U \not\subseteq \alpha$.

We have proved that $\mathrm{M}_{\mathbf{A}}(\alpha, \beta) \subseteq \mathrm{N}_{\mathbf{A}}(\alpha, \beta)$. Since obviously $\mathrm{N}_{\mathbf{A}}(\alpha, \beta) \subseteq \mathrm{U}_{\mathbf{A}}(\alpha, \beta)$, the minimal members of $\mathrm{U}_{\mathbf{A}}(\alpha, \beta)$ have to be minimal in $\mathrm{N}_{\mathbf{A}}(\alpha, \beta)$, which finishes the proof. □

2.4 Lemma. *Let* $\mathbf{A}$ *be a finite algebra and* $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, $\alpha \prec \beta$. *For each* $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $\alpha|_U \prec \beta|_U$ *in* $\mathrm{Con}\,\mathbf{A}|_U$.

Proof. By Theorem 2.3, there exists $e \in \mathrm{E}(\mathbf{A})$ with $U = e(A)$ and $e(\beta) \not\subseteq \alpha$. As in the proof of that theorem, we get that $\alpha|_U = e(\alpha)$ and $\beta|_U = e(\beta)$. Since $e(\alpha) \subseteq \alpha$, it follows that $\alpha|_U < \beta|_U$. Suppose for contradiction that there exists $\sigma \in \mathrm{Con}\,\mathbf{A}|_U$ such that $\alpha|_U < \sigma < \beta|_U$. Define

$$\theta = \{\langle x, y\rangle \in \beta : \langle eg(x), eg(y)\rangle \in \sigma \text{ for all } g \in \mathrm{Pol}_1 \mathbf{A}\}.$$

Obviously, θ is an equivalence relation on A. Let $\langle x, y\rangle \in \theta$ and $f \in \mathrm{Pol}_1 \mathbf{A}$ be arbitrary. For every $g \in \mathrm{Pol}_1 \mathbf{A}$,

$$\langle eg(f(x)), eg(f(y))\rangle = \langle e(gf)(x), e(gf)(y)\rangle \in \sigma.$$

Thus $\langle f(x), f(y)\rangle \in \theta$, and so $\theta \in \operatorname{Con}\mathbf{A}$. Since $\alpha \leq \theta \leq \beta$, either $\theta = \alpha$ or $\theta = \beta$. To finish the proof, we will show that $\theta|_U = \sigma$, which contradicts $\alpha|_U < \sigma < \beta|_U$.

First, if $\langle x, y\rangle \in \theta|_U$, then $\langle x, y\rangle = \langle ee(x), ee(y)\rangle \in \sigma$ and thus $\theta|_U \subseteq \sigma$. Second, if $\langle x, y\rangle \in \sigma$ and $g \in \operatorname{Pol}_1\mathbf{A}$, then $eg|_U \in \operatorname{Pol}_1(\mathbf{A}|_U)$. This gives $\langle eg(x), eg(y)\rangle \in \sigma$ and consequently, $\sigma \subseteq \theta|_U$. □

2.5 Remark. Let $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) = U$. Since $e(\beta) = \beta|_U$, from the previous lemma it follows that in this case we always have $e(\beta) \not\subseteq \alpha$.

2.6 Definition. Let $\mathbf{A}$ be any algebra and let B and C be nonvoid subsets of $\mathbf{A}$. B and C are **polynomially isomorphic** in $\mathbf{A}$ ($B \simeq C$) iff there exist $f, g \in \operatorname{Pol}_1\mathbf{A}$ such that $f(B) = C$, $g(C) = B$ and

$$gf|_B = \mathrm{id}_B, \quad fg|_C = \mathrm{id}_C\,.$$

We write $f : B \simeq C$ iff $f \in \operatorname{Pol}_1\mathbf{A}$ and there exists $g \in \operatorname{Pol}_1\mathbf{A}$ such that the above equations hold.

2.7 Remark. For $\mathbf{A}$ finite it suffices to find $f, g \in \operatorname{Pol}_1\mathbf{A}$ such that f maps B onto C and g maps C onto B. Then $gf|_B$ is a permutation of finite set B, and therefore $(gf|_B)^k = \mathrm{id}_B$ for some $k \geq 1$. Thus we get $f : B \simeq C$ from the previous definition with the polynomial $(gf)^{k-1}g$ instead of g.

2.8 Excercise. Let B and C be nonvoid subsets of an algebra $\mathbf{A}$, $f : B \simeq C$. Then $f|_B$ is an isomorphism between the structures $\langle B, (\operatorname{Pol}\mathbf{A})|_B, \theta|_B\,(\theta \in \operatorname{Con}\mathbf{A})\rangle$ and $\langle C, (\operatorname{Pol}\mathbf{A})|_C, \theta|_C\,(\theta \in \operatorname{Con}\mathbf{A})\rangle$.

Proof. From the definition, there is $g \in \operatorname{Pol}_1\mathbf{A}$ such that $gf|_B = \mathrm{id}_B$, $fg|_C = \mathrm{id}_C$. Clearly, $f|_B$ is a bijection of B onto C. First we will deal with the congruences. Let $\theta \in \operatorname{Con}\mathbf{A}$ be arbitrary. To prove that $f|_B$ is an isomorphism, we will show that $f(\theta|_B) = \theta|_C$, and therefore also $g(\theta|_C) = gf(\theta|_B) = \theta|_B$. For any $\langle x, y\rangle \in \theta|_B$, we have that $\langle f(x), f(y)\rangle \in \theta|_C$. Symmetrically, for $\langle x', y'\rangle \in \theta|_C$, $\langle g(x'), g(y')\rangle \in \theta|_B$.

Now, for each $\pi \in (\operatorname{Pol}\mathbf{A})|_B$, $\pi = h|_B$ for some $h \in \operatorname{Pol}\mathbf{A}$ (let h be n-ary), B closed under h. Consider the polynomial h' defined as

$$h'(x_0, x_1, \ldots, x_{n-1}) = f(h(g(x_0), g(x_1), \ldots, g(x_{n-1}))).$$

Obviously, $h' \in \operatorname{Pol}\mathbf{A}$ and C is closed under h'. To prove that $f|_B$ is an isomorphism, it remains to check that

$$f(h(x_0, x_1, \ldots, x_{n-1})) = h'(f(x_0), f(x_1), \ldots, f(x_{n-1}))),$$

which is easy. □

2.2 Properties of minimal sets

Let $\mathbf{A}$ be a finite algebra. The relation "to be polynomially isomorphic" ($\simeq$) is an equivalence relation on the power set of A. It is not hard to see that if $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $U \simeq V$, then also $V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. In the next theorem, assertion (2), we will prove the other implication. Therefore we will see that $\mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, the set of $\langle \alpha, \beta \rangle$-minimal sets of $\mathbf{A}$, is equal to certain equivalence class of $\simeq$.

The following theorem is one of the essential theorems in tame congruence theory.

2.9 Theorem (Properties of minimal sets). *Let $\mathbf{A}$ be a finite algebra and $\alpha, \beta \in \operatorname{Con}\mathbf{A}$, $\alpha \prec \beta$. The following statements hold.*

(1) For each $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, β is the transitive closure of

$$\alpha \cup \bigcup_{g \in \operatorname{Pol}_1 \mathbf{A}} g(\beta|_U) \stackrel{\text{def}}{=} \alpha \cup \{\langle g(x), g(y)\rangle : \langle x, y\rangle \in \beta|_U \text{ and } g \in \operatorname{Pol}_1 \mathbf{A}\}.$$

(2) For all $U, V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $U \simeq V$.

(3) If $\langle x, y\rangle \in \beta - \alpha$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, then there exists $f \in \operatorname{Pol}_1 \mathbf{A}$ such that $f(A) = U$ and $\langle f(x), f(y)\rangle \in \beta|_U - \alpha|_U$.

(4) For all $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f \in \operatorname{Pol}_1 \mathbf{A}$, if $f(\beta|_U) \not\subseteq \alpha$ then $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f : U \simeq f(U)$.

(5) If $f \in \operatorname{Pol}_1 \mathbf{A}$, $f(\beta) \not\subseteq \alpha$ then for some $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, $f : U \simeq f(U)$.

Proof.

(1) Denote by T the given set and let $\Theta(T)$ be its transitive closure. It is easily seen that $\Theta(T) \in \operatorname{Con}\mathbf{A}$ and $\alpha \leq \Theta(T) \leq \beta$. To prove $\alpha < \Theta(T)$ it suffices to show that $\alpha \subsetneqq T$.

By Theorem 2.3 there exists $e \in \mathrm{E}(\mathbf{A})$ such that $U = e(A)$. Since $e|_U = \mathrm{id}_U$, we have that

$$e(\beta|_U) = \beta|_U \not\subseteq \alpha$$

(see Lemma 2.4), which proves $\alpha \subsetneqq T$. Thus we conlude $\Theta(T) = \beta$.

(2) Choose arbitrary $U, V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. By Theorem 2.3 there exists $e \in \mathrm{E}(\mathbf{A})$ such that $U = e(A)$. From the definition of $V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ we have $V = f(A)$ for some $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\beta) \not\subseteq \alpha$. We shall find $\mu \in \mathrm{Pol}_1 \mathbf{A}$ such that $\mu(U) = V$.

By (1), β is the transitive closure of $\alpha \cup \bigcup_{g \in \mathrm{Pol}_1 \mathbf{A}} g(\beta|_U)$. Since $f(\beta) \not\subseteq \alpha$ and $f(\alpha) \subseteq \alpha$, there must exist $g \in \mathrm{Pol}_1 \mathbf{A}$ such that $fg(\beta|_U) \not\subseteq \alpha$, i.e. there exists $a, b \in U$, $\langle a, b\rangle \in \beta$ but $\langle fg(a), fg(b)\rangle \notin \alpha$. Since $e|_U = \mathrm{id}_U$, we have that

$$\langle fge(a), fge(b)\rangle = \langle fg(a), fg(b)\rangle \notin \alpha$$

We define $\mu = fge$. We see that $\mu \in \mathrm{Pol}_1 \mathbf{A}$, $\mu(A) \subseteq V$ and $\mu(\beta) \not\subseteq \alpha$. Thus by the $\langle \alpha, \beta\rangle$-minimality of V we get $\mu(A) = V$. Now we have

$$V = \mu(A) = fge(A) = fgee(A) = fge(U) = \mu(U)$$

Symmetrically, there exists $\nu \in \mathrm{Pol}_1 \mathbf{A}$, $\nu(V) = U$. Since A is finite, it follows from Remark 2.7 that $U \simeq V$.

(3) From Theorem 2.3 we have that $U = e(A)$ for some $e \in \mathrm{E}(A)$. We define

$$\theta = \{\langle x, y\rangle \,:\, \langle eg(x), eg(y)\rangle \in \alpha \text{ for all } g \in \mathrm{Pol}_1 \mathbf{A}\}$$

We see that $\theta \in \mathrm{Con}\,\mathbf{A}$, $\alpha \leq \theta \leq \beta$. From $ee(\beta) = e(\beta) \not\subseteq \alpha$ it follows that there exists $\langle x, y\rangle \in \beta$ such that $\langle ee(x), ee(y)\rangle \notin \alpha$, which proves $\theta < \beta$. Hence $\theta = \alpha$.

Now fix $\langle x, y\rangle \in \beta - \alpha$. Since $\langle x, y\rangle \notin \theta$, there exists $g \in \mathrm{Pol}_1 \mathbf{A}$ such that $\langle eg(x), eg(y)\rangle \notin \alpha$. We define $f = eg$. Since $f(\beta) \not\subseteq \alpha$ and

$$f(A) = eg(A) \subseteq e(A) = U$$

It follows by the $\langle \alpha, \beta\rangle$-minimality of U that $f(A) = U$. We have that $\langle f(x), f(y)\rangle \in \beta|_U - \alpha|_U$ and (4) is proved.

(4) Choose $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\beta|_U) \not\subseteq \alpha$. By Theorem 2.3 there is $e \in \mathrm{E}(A)$, $U = e(A)$. Thus we have that $fe(\beta) \not\subseteq \alpha$. Let $\langle a, b\rangle \in \beta$ be such that $\langle fe(a), fe(b)\rangle \notin \alpha$. By applying (3) on U and $\langle fe(a), fe(b)\rangle \in \beta - \alpha$ we obtain $g \in \mathrm{Pol}_1 \mathbf{A}$ such that $g(A) = U$ and $\langle gfe(a), gfe(b)\rangle \in \beta|_U - \alpha|_U$. It follows that $gfe(\beta) \not\subseteq \alpha$ and by the $\langle \alpha, \beta\rangle$-minimality of U

$$U = gfe(A) = gf(U)$$

(i.e., g maps $f(U)$ onto U). Since A is finite, it follows that $f : U \simeq f(U)$ (see Remark 2.7). As an easy corollary of this we get $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, which finishes the proof of (4).

(5) Choose $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\beta) \not\subseteq \alpha$. Let $V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ be arbitrary. By (1) for V there exists $f \in \mathrm{Pol}_1 \mathbf{A}$ such that $fg(\beta|_U) \not\subseteq \alpha$. By applying (4) for V and g it follows that $g(V) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. We define $U = g(V)$.

Since $fg(\beta|_V) \not\subseteq \alpha$, certainly $f(\beta|_U) \not\subseteq \alpha$ and (5) follows by an application of (4).

□

2.10 Excercise. A modified form of Theorem 2.9 (3) is valid:

(3') For each $\langle x, y\rangle \in \beta - \alpha$ there exists $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $e \in \mathrm{E}(\mathbf{A})$ such that $e(A) = U$ and $\langle e(x), e(y)\rangle \in \beta|_U - \alpha|_U$.

However, (3') can't be modified to read "For each $\langle x, y\rangle \in \beta - \alpha$ and $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ there exists $e \in \mathrm{E}(\mathbf{A})$ such that ...". There exists a three-element unary algebra for which this statement fails.

Proof. Choose $\langle x, y\rangle \in \beta - \alpha$ and let $V \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ be arbitrary. By Theorem 2.9 (3) there exists $f \in \mathrm{Pol}_1 \mathbf{A}$ such that $f(A) = V$ and $\langle f(x), f(y)\rangle \in \beta|_V - \alpha|_V$. Now, from Theorem 2.9 (1) it follows that there exist a sequence $x = x_0, x_1, \ldots, x_{n-1}, x_n = y$ of elements of A such that for each $0 < i \leq n$, $\langle x_{i-1}, x_i\rangle \in \alpha$ or $\langle x_{i-1}, x_i\rangle \in g_i(\beta|_V)$ for some $g_i \in \mathrm{Pol}_1 \mathbf{A}$.

Since $\langle f(x), f(y)\rangle \notin \alpha$, not all of the tuples $\langle f(x_{i-1}), f(x_i)\rangle$ are in α; and so we get that $fg(\beta|_V) \not\subseteq \alpha$ for some $g \in \mathrm{Pol}_1 \mathbf{A}$. It follows that $fg(V) = V$, fg is a permutation of the finite set V; and so $(fg)^k|_V = \mathrm{id}_V$ for some $k > 0$.

We define $U = g(V)$ and $e = (gf)^k$. Since $g(\beta|_V) \not\subseteq \alpha$, it follows from Theorem 2.9 (4) that $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Let $z \in A$ be arbitrary. We have that

$$e^2(z) = g(fg)^{2k-1}(f(z)) = g(fg)^{k-1}(f(z)) = e(z),$$

which proves $e \in \mathrm{E}(\mathbf{A})$. It is now easily seen that $e(A) = U$ and $\langle e(x), e(y)\rangle \in \beta|_U - \alpha|_U$.

To construct the counter-example, consider a three-element set $A = \{a, b, c\}$. Denote by U the subset $\{a, b\}$. We define three mappings $e, f, g : A \to A$ in the following way:

$$\begin{array}{lll} e(a) = a & e(b) = b & e(c) = b \\ f(a) = a & f(b) = b & f(c) = a \\ g(a) = a & g(b) = c & g(c) = b \end{array}$$

Let $\mathbf{A}$ be the algebra $\langle A, f, g\rangle$. We see that $\mathbf{A}$ has only the trivial congruences $0_A, 1_A$ (for example, if $\alpha \in \operatorname{Con}\mathbf{A}$ and $\langle a, b\rangle \in \alpha$ then $\langle a, c\rangle = \langle g(a), g(b)\rangle \in \alpha$ and by transitivity also $\langle b, c\rangle$; and so $\alpha = 1_A$). Since $U = f(A)$, we have that $U \in \mathrm{M}_{\mathbf{A}}(0_A, 1_A)$. We will prove that the statement fails for the tuple $\langle a, c\rangle \in 1_A - 0_A$ (i.e., $a \neq c$).

It is easily seen that e is the only idempotent satisfying $e(A) = U$ and $e(a) \neq e(c)$; therefore it suffices to prove that $e \notin \operatorname{Pol}_1 \mathbf{A}$. Every $h \in \operatorname{Pol}_1 \mathbf{A}$ is a composition of f's and g's. If we use f in this composition, two elements will map onto a and since $f(a) = g(a) = a$, the resulting operation will also map two elements onto a. On the other hand, if $h = g^k$ for some $k \geq 0$, then either $h = \mathrm{id}_A$, or $h = g$. In both cases we have $h \neq e$.

□

2.11 Excercise. Assumption (4) of Theorem 2.9 can be strengthened. If $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f \in \operatorname{Pol}_1 \mathbf{A}$, then $f(\beta|_U) \not\subseteq \alpha$ iff $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. However, if $f|_U$ is one-to-one it need not follow that $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. There is a three-element unary algebra for which the implication fails.

Proof. Let us have $f \in \operatorname{Pol}_1 \mathbf{A}$ such that $U, f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. From 2.9 (2) we have that $U \simeq f(U)$, let $g \in \operatorname{Pol}_1 \mathbf{A}$ be such that $gf|_U = \mathrm{id}_U$. Since

$$gf(\beta|_U) = \beta|_U \not\subseteq \alpha,$$

it follows that $f(\beta|_U) \not\subseteq \alpha$ and the strengthened version of 2.9 (4) is proved.

To construct the counter-example, let us have a three-element set $A = \{a, b, c\}$. Define two mappings $f, g : A \to A$ in the following way:

$$\begin{array}{lll} f(a) = a & f(b) = a & f(c) = c \\ g(a) = a & g(b) = a & g(c) = b \end{array}$$

Consider the algebra $\mathbf{A} = \langle A, f, g\rangle$. It is not hard to see that $\mathbf{A}$ has precisely three congruences, $0_A \prec \alpha \prec 1_A$, where $\alpha = 0_A \cup \{\langle a, b\rangle, \langle b, a\rangle\}$. Denote $U = \{a, c\}$. We have that $U = f(A)$, $f(1_A) \not\subseteq \alpha$, so $U \in \mathrm{U}_{\mathbf{A}}(\alpha, 1_A)$. The proper subsets of U are at most one-element, so they can't be in $\mathrm{U}_{\mathbf{A}}(\alpha, 1_A)$. Therefore U is an $\langle \alpha, 1_A\rangle$-minimal set.

Now, $g|_U$ is one-to-one, but $g(U) = \{a, b\}$ and $\langle a, b\rangle \in \alpha$, which implies that $g(U) \notin \mathrm{M}_{\mathbf{A}}(\alpha, 1_A)$. □

2.12 Excercise. Let $\mathbf{A}$ be a finite lattice, $\alpha, \beta \in \operatorname{Con}\mathbf{A}$, $\alpha \prec \beta$. Then every $\langle \alpha, \beta\rangle$-minimal set has precisely two elements.

Proof. First, we will prove that there exist $a, b \in \mathbf{A}$ such that $a \prec b$ and $\langle a, b\rangle \in \beta - \alpha$. Choose arbitrary $c, d \in \mathbf{A}$, $\langle c, d\rangle \in \beta - \alpha$.

Consider the unary polynomial $f(x) = x \vee c$. We have that $\langle f(c), f(d)\rangle = \langle c, c \vee d\rangle \in \beta$. In the same way, by applying $g(x) = x \vee d$ we get that $\langle c \vee d, d\rangle \in \beta$. There exist $r_0, r_1, \ldots, r_n \in \mathbf{A}$ such that $c = r_0 \prec r_1 \prec \ldots \prec r_n = c \vee d$. It is easily seen that $\langle r_{i-1}, r_i\rangle \in \beta$ for $1 \leq i \leq n$. Analogously, there exist $s_0, s_1, \ldots, s_m \in \mathbf{A}$, $d = s_0 \prec s_1 \prec \ldots \prec s_m = c \vee d$ and $\langle s_{j-1}, s_j\rangle \in \beta$, $1 \leq j \leq m$. Since $\langle c, d\rangle \notin \alpha$, it follows by transitivity of α that at least one of the tuples $\langle r_{i-1}, r_i\rangle$ or $\langle s_{j-1}, s_j\rangle$ (which are all prime quotients in $\mathbf{A}$) is not in α.

Finally, let $a, b \in \mathbf{A}$ be such that $a \prec b$ and $\langle a, b\rangle \in \beta - \alpha$. Consider the unary polynomial $h(x) = (x \wedge b) \vee a$. We have that $h(A) = \{a, b\}$ and $\langle h(a), h(b)\rangle = \langle a, b\rangle \in \beta - \alpha$, which implies $h(\beta) \not\subseteq \alpha$. Thus $\{a, b\} \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and the rest follows from 2.9 (2). □

2.3 Trace and body

2.13 Definition. Let $\mathbf{C}$ be a finite algebra.

a) Let $\delta, \theta \in \operatorname{Con}\mathbf{C}$, $\delta \prec \theta$. $\mathbf{C}$ is called $\langle \delta, \theta\rangle$-**minimal** iff $C \in \mathrm{M}_{\mathbf{C}}(\delta, \theta)$.

b) C is called **minimal** iff $|C| > 1$ and every non-constant $f \in \operatorname{Pol}_1\mathbf{C}$ is a permutation of $\mathbf{C}$.

From the next lemma it follows that a simple finite algebra $\mathbf{C}$ is minimal iff it is $\langle 0_C, 1_C\rangle$-minimal.

2.14 Lemma. *Let* $\mathbf{A}$ *be a finite algebra,* $\delta, \theta \in \operatorname{Con}\mathbf{A}$*,* $\delta \prec \theta$*.*

(1) $\mathbf{A}$ *is* $\langle \delta, \theta \rangle$*-minimal iff for all* $f \in \mathrm{Pol}_1 \mathbf{A}$ *either* f *is a permutation of* A *or* $f(\theta) \subseteq \delta$.

(2) If $U \in \mathrm{M}_{\mathbf{A}}(\delta, \theta)$*, then the algebra* $\mathbf{A}|_U$ *is* $\langle \delta|_U, \theta|_U \rangle$*-minimal.*

Proof.

(1) $\Rightarrow$: Suppose $\mathbf{A} \in \mathrm{M}_{\mathbf{A}}(\delta, \theta)$. Let $f \in \mathrm{Pol}_1 \mathbf{A}$ be such that $f(\theta) \not\subseteq \delta$. Then $f(A) \in \mathrm{U}_{\mathbf{A}}(\delta, \theta)$ and, by the $\langle \delta, \theta \rangle$-minimality of A, $f(A) = A$. A is finite, therefore f is a permutation of A.

$\Leftarrow$: We have that $A = \mathrm{id}(A)$ and $\mathrm{id}(\theta) = \theta \not\subseteq \delta$, thus $A \in \mathrm{U}_{\mathbf{A}}(\delta, \theta)$. Moreover, for any $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\theta) \not\subseteq \delta$, implies $f(A) = A$. Since A is the only member of $\mathrm{U}_{\mathbf{A}}(\delta, \theta)$, it is minimal.

(2) Let $g \in \mathrm{Pol}_1 \mathbf{A}|_U$ be arbitrary. From the definition, $g = f|_U$ for some $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(U) \subseteq U$. Suppose that $f(\theta|_U) \not\subseteq \delta|_U$. We know that $U = e(A)$ for some $e \in \mathrm{E}(\mathbf{A})$. Since $e(\theta) = \theta|_U$, we get

$$fe(\theta) = f(\theta|_U) \not\subseteq \delta|_U,$$

which implies $fe(\theta) \not\subseteq \delta$. We have that $fe(A) = f(U) \subseteq U$, therefore $f(U) = U$ (by the $\langle \delta, \theta \rangle$-minimality of U). Now (2) follows by an application of (1) to the algebra $\mathbf{A}|_U$.

□

2.15 Definition.

a) Let $\mathbf{C}$ be $\langle \delta, \theta \rangle$-minimal. A subset $N \subseteq C$ is called a $\langle \delta, \theta \rangle$-**trace** in $\mathbf{C}$ iff N is a θ-class which contains at least two δ-classes (i.e., $N = x/\theta$ for some $x \in C$ such that $x/\theta \neq x/\delta$).

The **body** of $\mathbf{C}$ is the union of its $\langle \delta, \theta \rangle$-traces.

The **tail** of $\mathbf{C}$ is the complement of its body in C.

b) Let $\mathbf{A}$ be a finite algebra. By an $\langle \alpha, \beta \rangle$-**trace** in $\mathbf{A}$ we mean a subset $N \subseteq A$ such that for some $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$, N is an $\langle \alpha|_U, \beta|_U \rangle$-trace of the algebra $\mathbf{A}|_U$ (i.e., for some $x \in U$, $N = x/(\beta|_U) \neq x/(\alpha|_U)$).

By Theorem 2.9 (2), all $\langle \alpha, \beta \rangle$-minimal sets are polynomially isomorphic. It is easy to see that this isomorphism preserves the property "being a trace" (and the same is true for body and tail). Therefore, each $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$

contains a full representative set of traces with respect to the equivalence relation $\simeq$.

From Lemma 2.4 it follows that $\mathbf{C}$ has at least one trace (i.e., the body of $\mathbf{C}$ is always nonempty). The following theorem tells us that each β-class is actually "connected" by the traces it contains.

2.16 Theorem. *Let $\mathbf{A}$ be a finite algebra and $\alpha, \beta \in \operatorname{Con}\mathbf{A}$, $\alpha \prec \beta$. Define the relation*

$$\rho = \alpha \cup \bigcup \{N^2 \,:\, N \text{ is an } \langle\alpha,\beta\rangle\text{-trace}\}.$$

Then β is the transitive closure of ρ.

Proof. Obviously, $\rho \subseteq \beta$. Choose any $U \in \mathrm{M}_{\mathbf{A}}(\alpha,\beta)$. By 2.9 (1), β is the transitive closure of $\rho' = \alpha \cup \{\langle g(x), g(y)\rangle \,:\, \langle x,y\rangle \in \beta|_U \text{ and } g \in \operatorname{Pol}_1\mathbf{A}\}$. To prove the statement, it suffices to show $\rho' \subseteq \rho$.

Choose arbitrary $g \in \operatorname{Pol}_1\mathbf{A}$ and $\langle x,y\rangle \in \beta|_U$. Suppose $\langle g(x), g(y)\rangle \notin \alpha$. We see that $\langle x,y\rangle \notin \alpha|_U$ and $N = x/(\beta|_U)$ is an $\langle\alpha,\beta\rangle$-trace. From 2.9 (4) it follows that $g(U) \in \mathrm{M}_{\mathbf{A}}(\alpha,\beta)$ and $g : U \simeq g(U)$. Therefore $g(N)$ is also an $\langle\alpha,\beta\rangle$-trace. Now $\langle x,y\rangle \in N$ implies $\langle g(x),(y)\rangle \in g(N) \subseteq \rho$, which finishes the proof. □

2.17 Lemma. *Let $\alpha \leq \delta \prec \theta$ be congruences of a finite algebra $\mathbf{C}$. Suppose that $\mathbf{C}$ is $\langle\delta,\theta\rangle$-minimal and N is a $\langle\delta,\theta\rangle$-trace.*

(1) The quotient algebra $\mathbf{C}/\alpha$ is $\langle\delta/\alpha,\theta/\alpha\rangle$-minimal.

(2) $\mathbf{C}|_N$ is $\langle\delta|_N, 1|_N\rangle$-minimal.

(3) $(\mathbf{C}|_N)/\delta|_N$ is a minimal algebra isomorphic to $\mathbf{C}/\delta|_{N/\delta}$.

Proof. We see that $\delta/\alpha \prec \theta/\alpha$. Since N is a $\langle\delta,\theta\rangle$-trace, we have that $\delta|_N \prec 1|_N$. Thus everything in the statement is correctly defined.

(1) Recall that $\operatorname{Pol}_1\mathbf{C}/\alpha = \{f_\alpha \,:\, f \in \operatorname{Pol}_1\mathbf{C}\}$ (see Lemma 1.7). Choose arbitrary $f_\alpha \in \operatorname{Pol}_1\mathbf{C}/\alpha$. It is easily seen that $f(\theta) \not\subseteq \delta$ iff $f_\alpha(\theta/\alpha) \not\subseteq \delta/\alpha$.

Suppose that $f_\alpha(\theta/\alpha) \not\subseteq \delta/\alpha$. Then we have that $f(\theta) \not\subseteq \delta$ and by Lemma 2.14 (1), f is a permutation of C. Since $f(C) = C$, we also have that $f_\alpha(\mathbf{C}/\alpha) = \mathbf{C}/\alpha$. To finish the proof, apply Lemma 2.14 (1) to $\mathbf{C}/\alpha$.

(2) Let $f \in \mathrm{Pol}_1(\mathbf{C}|_N)$ and suppose that $f(N^2) = f(1_N) \not\subseteq \delta|_N$. There exists $g \in \mathrm{Pol}_1 \mathbf{C}$ with $f = g|_N$, $g(N) \subseteq N$. Since N is a $\langle \delta, \theta \rangle$-trace, $N^2 \subseteq \theta$. Thus we have that for some $\langle x, y \rangle \in \theta$, the tuple $\langle g(x), g(y) \rangle$ is contained in N^2 and not in $\delta|_N$. Therefore $\langle g(x), g(y) \rangle \notin \delta$; and so $g(\theta) \not\subseteq \delta$, which implies that g is a permutation of C. It follows that $f = g|_N$ is injective, therefore it is a permutation of the finite set N. Using Lemma 2.14 (1), we conclude that $\mathbf{C}|_N$ is $\langle \delta|_N, 1|_N \rangle$-minimal.

(3) We have that $\delta|_N \leq \delta|_N \prec 1_N$. Using statement (1) we conclude that $(\mathbf{C}|_N)/\delta|_N$ is $\langle 0_{(C|_N)/\delta|_N}, 1_{(C|_N)/\delta|_N} \rangle$-minimal; and so it is minimal. It is easy to see that $(\mathbf{C}|_N)/\delta|_N \simeq (\mathbf{C}/\delta)|_{N/\delta}$ since $\delta \subseteq \theta$ and N is a θ-class.

□

2.18 Theorem. *Let $\delta \leq \alpha \prec \beta$ be congruences of a finite algebra $\mathbf{A}$. Then*

$$\mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta) = \mathrm{M}_{\mathbf{A}}(\alpha, \beta)/\delta \stackrel{\mathrm{def}}{=} \{U/\delta \,:\, U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)\}.$$

Moreover, for any $\langle \alpha, \beta \rangle$-minimal set U, the $\langle \alpha/\delta, \beta/\delta \rangle$-traces in U/δ are precisely the sets N/δ where N is an $\langle \alpha, \beta \rangle$-trace in U.

Proof. Choose any $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. By Theorem 2.3, there is $e \in \mathrm{E}(\mathbf{A})$ with $U = e(A)$. Recall that $\mathrm{Pol}\,\mathbf{A}/\delta = \{f_\delta \,:\, f \in \mathrm{Pol}\,\mathbf{A}\}$ and that for any $f \in \mathrm{Pol}_1 \mathbf{A}$, $f(\beta) \not\subseteq \alpha$ iff $f_\delta(\beta/\delta) \not\subseteq \alpha/\delta$.

First, note that $e_\delta \in \mathrm{E}(\mathbf{A}/\delta)$, $U/\delta = e_\delta(A/\delta)$ and $e_\delta(\beta/\delta) \not\subseteq \alpha/\delta$. Thus, $U/\delta \in \mathbf{A}/\delta$. Second, let f_δ ($f \in \mathrm{Pol}_1 \mathbf{A}$) be any unary polynomial of $\mathbf{A}/\delta$ such that $f_\delta(A/\delta) \subseteq U/\delta$ and $f_\delta(\beta/\delta) \not\subseteq \alpha/\delta$. Notice that $f_\delta = e_\delta \circ f_\delta = (ef)_\delta$, and so $ef(\beta) \not\subseteq \alpha$. Thus $ef(A) = U$, $f_\delta(\mathbf{A}/\delta) = (ef)_\delta(\mathbf{A}/\delta) = U/\delta$ and we conclude that $U/\delta \in \mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$.

Now, let W be any member of $\mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$. Choose arbitrary $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Since $U/\delta \in \mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta)$, by Theorem 2.9 (2) there is f_δ ($f \in \mathrm{Pol}_1 \mathbf{A}$) with $f_\delta : U/\delta \simeq W$. In this situation, we have that $f_\delta((\beta/\delta)|_{U/\delta}) \not\subseteq \alpha/\delta$ (see Excercise 2.11). Thus $f(\beta|_U) \not\subseteq \alpha$ and by Theorem 2.9 (4), $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. Now, $W = f_\delta(U/\delta) = f(U)/\delta$ which proves $W \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)/\delta$.

We have proved that $\mathrm{M}_{\mathbf{A}/\delta}(\alpha/\delta, \beta/\delta) = \mathrm{M}_{\mathbf{A}}(\alpha, \beta)/\delta$. The rest of the statement now follows easily. □

2.19 Excercise. Let $\mathbf{A}$ be a finite algebra and $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, $\alpha \prec \beta$. Suppose that N is an $\langle \alpha, \beta \rangle$-trace in $\mathbf{A}$ and that $f \in \mathrm{Pol}_1 \mathbf{A}$. Prove that either $f(N^2) \subseteq \alpha$, or $f(N)$ is an $\langle \alpha, \beta \rangle$-trace and $f : N \simeq f(N)$.

Proof. If $f(N^2) \subseteq \alpha$, then obvisouly $f(N)$ is not an $\langle \alpha, \beta \rangle$-trace. Suppose that $f(N^2) \nsubseteq \alpha$. Let $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ be such that N is an $\langle \alpha|_U, \beta|_U \rangle$-trace of $\mathbf{A}|_U$. Since $N^2 \subseteq \beta|_U$, we have that $f(\beta|_U) \nsubseteq \alpha$. By Theorem 2.9, $f(U) \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$ and $f : U \simeq f(U)$. If $N = x/(\beta|_U)$, then

$$f(N) = f(x)/f(\beta|_U) = f(x)/(\beta|_{f(U)}) \neq f(x)/(\alpha|_{f(U)}).$$

The rest is obvious (see Excercise 2.8). □

Chapter 3

The structure of minimal algebras

3.1 Polynomial operations

3.1 Definition. Let A be any set and $f : A^n \to A$ for some $n > 0$, $f = f(x_0, x_1, \ldots, x_{n-1})$. We say that f **depends on** x_i, where $0 \leq i < n$, iff there exist $a_j \in A$, $j \neq i$ such that $g(x) = f(a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{n-1})$ is not constant.

The following lemma is due to A. Salomaa:

3.2 Lemma. *Let* $\mathbf{A}$ *be an algebra and* $n > 0$. *Suppose that* $\mathbf{A}$ *has a polynomial operation that depends on at least* n *variables. Then for each* k, $1 \leq k \leq n$, *there exists* $f \in \mathrm{Pol}_k \mathbf{A}$ *that depends on all* k *variables.*

Proof. Let $g \in \mathrm{Pol}_m \mathbf{A}$ be such an operation. It is easy to see that if we substitute an arbitrary constant for each variable that g doesn't depend on, we get an operation that depends on all of its variables. Therefore we can suppose that $g \in \mathrm{Pol}_n \mathbf{A}$ and $g = g(x_0, x_1, \ldots, x_{n-1})$ depends on all its variables.

For each $0 \leq i < n$ and $a \in A$ we define an $(n-1)$-ary polynomial operation $g[a, i]$ in the following way:

$$g[a, i](x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n-1}) \stackrel{\text{def}}{=} (x_0, x_1, \ldots, x_{i-1}, a, x_{i-1}, \ldots, x_{n-1}).$$

We also define

$$\mathrm{D}(a, i) \stackrel{\text{def}}{=} \{j : j \neq i,\ g[a, i] \text{ depends on } x_i\}.$$

Let $0 \leq l < n$ be arbitrary. Choose $i < n$ and $a \in A$ such that $l \in \mathrm{D}(a, i)$ and $|\mathrm{D}(a, i)|$ is maximal. We claim that $j \in \mathrm{D}(a, i)$ for all $j < n, j \neq i$.

Suppose for contradiction that there exists $j \neq i$, $j \notin \mathrm{D}(a, i)$. Since g depends on x_i, we can choose $b \in A$ with $i \in \mathrm{D}(b, j)$. Let $i_0 \in \mathrm{D}(a, i)$ be arbitrary. We have that $g[a, i]$ doesn't depend on x_j, and therefore $g[b, j]$ depends on x_{i_0}. Now $\{i\} \cup \mathrm{D}(a, i) \subseteq \mathrm{D}(b, j)$, which contradicts the choice of a and i.

We have proved that $g[a, i] \in \mathrm{Pol}_{n-1} \mathbf{A}$ depends on all its $n-1$ variables. We can now continue by induction. □

3.3 Definition. Let A be any set and $f : A^n \to A$ for some $n \geq 0$. For each $0 \leq i < n$ and $k \geq 0$ we define an n-ary operation $f^k_{(i)}(x_0, x_1, \ldots, x_{n-1})$ on A in the following way:

$$f^0_{(i)}(x_0, x_1, \ldots, x_{n-1}) = x_i,$$
$$f^1_{(i)}(x_0, x_1, \ldots, x_{n-1}) = f(x_0, x_1, \ldots, x_{n-1})$$

and if $f^k_{(i)}$ is defined,

$$f^{k+1}_{(i)}(x_0, \ldots, x_{n-1}) = f(x_0, \ldots, x_{i-1}, f^k_{(i)}(x_0, \ldots, x_{n-1}), x_{i+1}, \ldots, x_{n-1}).$$

3.4 Lemma. *Let A be a finite set and $f : A^n \to A$ for some $n \geq 0$. There exists $k > 0$ such that*

$$\begin{aligned} f^k_{(i)}(x_0, \ldots, x_{n-1}) &= f^{2k}_{(i)}(x_0, \ldots, x_{n-1}) \\ &= f^k_{(i)}(x_0, \ldots, x_{i-1}, f^k_{(i)}(x_0, \ldots, x_{n-1}), x_{i+1}, \ldots, x_{n-1}) \end{aligned}$$

for all $x_0, \ldots, x_{n-1} \in A$ and $0 \leq i < n$.

Proof. This lemma is an easy corollary of Lemma 1.5. Let $k > 0$ be such that $g^k = g^{2k}$ for all $g : A \to A$. Choose $x_0, \ldots, x_{n-1} \in A$ and $0 \leq i < n$ and put

$$g(x) \stackrel{\mathrm{def}}{=} f(x_0, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{n-1})$$

for all $x \in A$. It is easy to prove by induction that for all $r > 0$

$$g^r(x) = f^r_{(i)}(x_0, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{n-1})$$

and thus also

$$g^{2r} = f^r_{(i)}(x_0, \ldots, x_{i-1}, f^r_{(i)}(x_0, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_{n-1}), x_{i+1}, \ldots, x_{n-1}).$$

Since $g^k = g^{2k}$, the assertion of this lemma is now obvious. □

3.2 The types of minimal algebras

3.5 Definition. A ternary operation $\varphi(x, y, z)$ on a set A is called a **Mal'cev operation** iff $\varphi(x, x, y) = \varphi(y, x, x) = y$ for all $x, y \in A$. An algebra $\mathbf{A}$ is called **Mal'cev** iff it has a Mal'cev term operation $\varphi \in \mathrm{Clo}_3 \mathbf{A}$.

3.6 Example. Let $\mathbf{G} = \langle G, \cdot \rangle$ be a group. Then $\varphi(x, y, z) = x \cdot y^{-1} \cdot z$ is a Mal'cev operation, and thus $\mathbf{G}$ is Mal'cev.

3.7 Definition. An algebra $\langle A, q \rangle$ with one binary operation q is called a **quasigroup** iff for all $a, c \in A$ there exist unique $x, y \in A$ such that $q(x, c) = a$ and $q(c, x) = a$.

3.8 Lemma. *Every finite quasigroup is Mal'cev.*

Proof. The idea of the proof is to construct a Mal'cev operation similar to the one in the example above. Let $\mathbf{A} = \langle A, q \rangle$ be a finite quasigroup. We want to find $u, v \in \mathrm{Pol}_2 \mathbf{A}$ such that $q(u(x, y), y) = x$ and $q(x, v(x, y)) = y$. The operations u and v are sometimes called *right* and *left division*, respectively. We will construct the Mal'cev operation φ from u and v in such a way that if $\mathbf{A}$ was a group, then $\varphi(x, y, z)$ would be equal to $x \cdot y^{-1} \cdot z$.

Let $k > 0$ be such that $q^k_{(0)}(x, y) = q^{2k}_{(0)}(x, y) = q^k_{(0)}(q^k_{(0)}(x, y), y)$ (see Lemma 3.4). We can obviously suppose $k > 1$. Since $\mathbf{A}$ is a quasigroup, for each $y \in A$ the function $f(x) = q(x, y)$ is a permutation of A. It follows that the function $f'(x) = q^k_{(0)}(x, y) = q(\ldots q(q(x, y), y), \ldots, y)$ is also a permutation (since it is a composition of permutations). From $q^k_{(0)} = q^{2k}_{(0)}$ (i.e., $f'(x) = f'(f'(x))$) we get that x is a fixed point of f', hence $q^k_{(0)}(x, y) = x$.

We define $u(x, y) = q^{k-1}_{(0)}(x, y)$. Then $q(u(x, y), y) = x$ for all $x, y \in A$. Repeating the same argument with x held fixed and y as a variable we obtain $v \in \mathrm{Pol}_2 \mathbf{A}$ which satisfies $q(x, v(x, y)) = y$ for all $x, y \in A$. Finally, we define

$$\varphi(x, y, z) = q(u(x, v(y, y)), v(y, z)).$$

Since $q(x, v(x, x)) = x$ and $q(u(x, v(x, x)), v(x, x)) = x$, it follows from the properties of the quasigroup operation q that $u(x, v(x, x)) = x$; and so $\varphi(x, x, y) = y$. We have that $\varphi(y, x, x) = q(u(y, v(x, x)), v(x, x)) = y$. Thus we have proved that φ is a Mal'cev operation. □

Recall that a finite algebra $\mathbf{M}$ is *minimal* iff $|M| \geq 2$ and every non-constant $f \in \mathrm{Pol}_1 \mathbf{M}$ is a permutation of M. We denote the group of permutations of the set M by $\mathrm{Sym}\, M$.

3.9 Definition. Algebras $\mathbf{A}$ and $\mathbf{B}$ are **polynomially equivalent** iff they have the same universe and $\operatorname{Pol}\mathbf{A} = \operatorname{Pol}\mathbf{B}$.

3.10 Lemma. *Let* $\mathbf{M}$ *be a minimal algebra. If each* $f \in \operatorname{Pol}\mathbf{M}$ *depends on at most one variable, then* $\mathbf{M}$ *is polynomially equivalent to the algebra* $\langle M, \Pi\rangle$ *for a subgroup* $\Pi \leq \operatorname{Sym} M$.

Proof. We define $\Pi = \operatorname{Pol}_1\mathbf{M} \cap \operatorname{Sym} M$. Let $n > 0$ and $f \in \operatorname{Pol}_n\mathbf{M}$ be arbitrary. If f is constant, then, of course, $f \in \operatorname{Pol}\langle M, \Pi\rangle$. Suppose that f is non-constant, thus it depends on exactly one variable. It follows that for some $0 \leq i < n$ and $\alpha \in \Pi$ we have $f(x_0, x_1, \ldots, x_{n-1}) = \alpha(x_i)$ for all $(x_0, x_1, \ldots, x_{n-1}) \in M^n$.

It remains to show that Π is a subgroup of $\operatorname{Sym} M$. We have $\mathrm{id}_M \in \Pi$ and obviously Π is closed under composition. Let $\beta \in \Pi$ be arbitrary. Since β is a permutation of finite M, there exists $k > 0$ such that $\beta^k = \mathrm{id}_M$. Now, $\beta^{k-1} \in \operatorname{Pol}_1\mathbf{M} \cap \operatorname{Sym} M = \Pi$; β^{k-1} is the permutation inverse to β. □

The following important theorem is due to P. P. Pálfy:

3.11 Theorem. *Let* $\mathbf{M}$ *be a minimal algebra of at least three elements. If there exists* $f \in \operatorname{Pol}\mathbf{M}$ *depending on more than one variable, then* $\mathbf{M}$ *is polynomially equivalent to a vector space over a finite field.*

Proof. Let $\mathbf{M}$ be minimal, $|M| \geq 3$ and let $\mathbf{M}$ have a polynomial operation depending on more than one variable. The proof proceeds through a series of assertions. The statements of the first two claims represent a weakened form of the definition of the *Abelian* property for general algebras (see Chapter 3 of [3]).

Claim 1. Let $f \in \operatorname{Pol}_2\mathbf{M}$ and $a, b, c, d \in$ M. Then $f(a, c) = f(a, d)$ implies $f(b, c) = f(b, d)$.

Suppose for contradiction that $f(a, c) = f(a, d)$ and $f(b, c) \neq f(b, d)$. Choose $k > 0$ such that the operation $g(x, y) = f^k_{(1)}(x, y)$ satisfies

$$g(x, y) = g^2_{(1)}(x, y) = g(x, g(x, y))$$

(see Lemma 3.4). We are going to find a contradiction based on the multiplication table of g. Since $\mathbf{M}$ is minimal, its rows and columns have to be either constant or permutations of M.

As the unary polynomial $h_1(x) = f(b, x)$ is not constant, it is a permutation of M. We have that $h^k_1(y) = h^{2k}_1(y)$, which implies $y = h^k_1(y)$. Thus

we have proved that $g(b, y) = y$ for all $y \in M$. On the contrary, since the polynomial $h_2(x) = g(a, x)$ is not a permutation, it must be constant. Let $e \in M$ be such that $g(a, y) = e$ for all $y \in M$.

Since $|M \geq 3|$, we can choose $z \in M$ such that $z \neq a, b$. We can also choose $w \in M$ with $w \neq e$. We have that $g(a, e) = e$ and $g(b, e) = e$, thus we conclude that $g(x, e) = e$ for all $x \in M$.

Now, consider the polynomial $h_3(x) = g(z, x)$. Either h_3 is constant, and thus $h_3(x) = g(z, x) = g(z, a) = e$ for all $x \in M$, or h_3 is a permutation. In that case we have that $h_3(x) = g(z, x) = g(z, g(z, x)) = h_3(h_3(x))$; and so $h_3(x) = x$ for all $x \in M$. We see that $g(z, w) \in \{e, w\}$.

Finally, take a look at $h_4(x) = g(x, w) \in \mathrm{Pol}_1 \mathbf{M}$. We see that $h_4(a) = e$, $h_4(b) = w$ and $h_4(z) \in \{e, w\}$. Thus h_4 is neither constant nor a permutation, which is a contradiction (see the the figure below).

	e	w
a	e	e
b	e	w
z	e	$g(z, w)$

Claim 2. Let $h \in \mathrm{Pol}_{n+1} \mathbf{M}$ for some $n > 0$ and $\bar{a}, \bar{b} \in M^n$ while $c, d \in \mathrm{M}$. Then $h(\bar{a}, c) = h(\bar{a}, d)$ implies $h(\bar{b}, c) = h(\bar{b}, d)$.

This follows easily by an application of Claim 1. Let $\bar{a} = (a_0, \ldots, a_{n-1})$ and $\bar{b} = (b_0, \ldots, b_{n-1})$. Consider the binary polynomial

$$g(x, y) = h(a_0, \ldots, a_{n-2}, x, y) \in \mathrm{Pol}_2 \mathbf{M}.$$

Since $g(a_{n-1}, c) = g(a_{n-1}, d)$, we have that $g(b_{n-1}, c) = g(b_{n-1}, d)$, which gives us

$$h(a_0, \ldots, a_{n-2}, b_{n-1}, c) = h(a_0, \ldots, a_{n-2}, b_{n-1}, d).$$

We continue in an obvious fashion by replacing a_{n-2} by b_{n-2} and so on; we end up with $h(\bar{b}, c) = h(\bar{b}, d)$.

Since $\mathbf{M}$ has a polynomial operation that depends on at least two variables, by Lemma 3.2 there exists $f \in \mathrm{Pol}_2 \mathbf{M}$ depending on both its variables.

Claim 3. The algebra $\langle M, f \rangle$ is a finite quasigroup.

Since $f(x, y)$ depends on y, we have that $f(c, y)$ (as a function of y) is not constant for some $c \in M$; and so there exist $a, b \in M$ with $f(c, a) \neq f(c, b)$. But then it follows from Claim 1 that $f(d, a) \neq f(d, b)$ for all $d \in M$.

For any $d \in M$, the unary polynomial $f(d, y)$ is not constant, and hence it is a permutation. Similarly, we have that $f(x, d)$ is a permutation for all $d \in M$ (we apply Claim 1 on the operation $f'(x, y) = f(y, x)$; notice that in the previous two claims we don't have to care about the order of variables). We conclude that $\langle M, f \rangle$ is a quasigroup.

From Claim 3 and Lemma 3.8 it follows that $\mathbf{M}$ has a Mal'cev operation, let us denote it by φ. We now choose one element of M, call it 0, and define the following operations:

$$x + y \stackrel{\text{def}}{=} \varphi(x, 0, y),$$
$$-x \stackrel{\text{def}}{=} \varphi(0, x, 0).$$

The Mal'cev operation $\varphi(x, y, z)$ turns out to be the same as $x - y + z$ in the vector space we are going to construct.

Claim 4. The algebra $\langle M, +, -, 0 \rangle$ is an Abelian group.

To prove the associative law, we define the following operation:

$$\delta(x, y, z, u) = \varphi(\varphi(x, 0, u), 0, \varphi(y, u, z)).$$

Notice that $\delta(0, b, 0, b) = \delta(0, b, 0, 0)$, and thus from Claim 2 it follows that $\delta(a, b, c, b) = \delta(a, b, c, 0)$. But we have that $\delta(a, b, c, b) = \varphi(\varphi(a, 0, b), 0, c) = (a + b) + c$ and $\delta(a, b, c, 0) = \varphi(a, 0, \varphi(b, 0, c)) = a + (b + c)$; and so the associative law is proved.

Now we define two more operations:

$$\delta_2(x, y) = \varphi(x, y, \varphi(y, x, 0)),$$
$$\delta_3(x, y, z) = \varphi(z, 0, \varphi(x, z, y)).$$

Since $\delta_2(a, 0) = \delta_2(0, 0)$, we get that $\delta_2(a, a) = \delta_2(a, 0)$ and hence $a + (-a) = \delta_2(a, 0) = \delta_2(a, a) = 0$. It is easy to see that $b + 0 = \varphi(b, 0, 0) = b$ for all $b \in M$.

It only remains to prove the commutative law. Notice that $\delta_3(0, 0, b) = b + (-b) = 0 = \delta_3(0, 0, 0)$, and therefore $\delta_3(a, b, b) = \delta_3(a, b, 0)$. Finally we have that $a + b = \delta_3(a, b, 0) = \delta_3(a, b, b) = b + a$.

Claim 5. If $h \in \mathrm{Pol}_n \mathbf{M}$ and $x_0, \ldots, x_{n-1} \in M$, then

$$h(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} h_i(x_i) - (n - 1) \cdot h(0, \ldots, 0)$$

where $h_i(x) = h(0, \ldots, 0, x, 0, \ldots, 0)$ (x occuring in the i-th place).

For $n = 1$ it is trivial. Let $n = 2$. We define the operation $g(x, y, z) = h(x, z) - h(y, z)$. Since obviously $h(0, y) - h(0, y) = h(0, 0) - h(0, 0)$, we get that $g(0, 0, y) = g(0, 0, 0)$. By Claim 2 it follows that $g(x, 0, y) = g(x, 0, 0)$; and so $h(x, y) = h(x, 0) + h(0, y) - h(0, 0)$.

The claim can now be proved for all $n > 2$ by induction. Assume that it holds for all $k < n$ and let $h \in \mathrm{Pol}_n \mathbf{M}$ be arbitrary. First, consider x_0 fixed. Then $h(x_0, x_1, \ldots, x_{n-1}) \in \mathrm{Pol}_{n-1} \mathbf{M}$ and the induction assumption gives

$$\begin{aligned} h(x_0, \ldots, x_{n-1}) = {} & h(x_0, x_1, 0, \ldots, 0) + h(x_0, 0, x_2, 0, \ldots, 0) + \cdots + \\ & + h(x_0, 0, \ldots, 0, x_{n-1}) - (n-2) \cdot h(x_0, 0, \ldots, 0). \end{aligned}$$

Now it suffices to rewrite each of $h(x_0, x_1, 0, \ldots, 0), \ldots, h(x_0, 0, \ldots, 0, x_{n-1})$ using the binary case of the claim; and the claim is proved.

We define F to be the set of all $\alpha \in \mathrm{Pol}_1 \mathbf{M}$ with $\alpha(0) = 0$. For $\alpha \in F$ we denote by $\alpha\cdot$ the unary operation $\alpha \cdot x = \alpha(x)$, $x \in M$. Let $\mathbf{F}$ be the algebra $\langle F, +, \circ \rangle$, where $\circ$ denotes composition of functions and $+$ pointwise addition.

Claim 6. $\mathbf{F}$ is a finite field, $\mathbf{V} = \langle M, +, -, 0, \alpha\cdot\ (\alpha \in F) \rangle$ is a vector space over $\mathbf{F}$ and $\mathrm{Pol}\,\mathbf{V} = \mathrm{Pol}\,\mathbf{M}$.

By applying Claim 5 to the operation $h(x, y) = \alpha(x + y)$ we get that

$$\alpha(x + y) = \alpha(x + 0) + \alpha(0 + y) - \alpha(0 + 0) = \alpha(x) + \alpha(y)$$

and thus α is an endomorphism of the group $\langle M, +, -, 0 \rangle$. Since F is closed under $\circ$ and $+$, it is a subring of the ring of all endomorphisms of $\langle M, +, -, 0 \rangle$.

Since $\mathbf{M}$ is minimal, we have for any $\alpha \in F$ that either α is identically zero, or it is a permutation of the finite set M. In that case there exists $k > 0$ such that $\alpha^k = \mathrm{id}_M$. Therefore each nonzero element of F has an inverse element in $\mathbf{F}$ and it follows that $\mathbf{F}$ is a field and $\mathbf{V}$ a vector space over $\mathbf{F}$.

It remains to prove that $\mathrm{Pol}\,\mathbf{V} = \mathrm{Pol}\,\mathbf{M}$. We see that $\mathrm{Pol}\,\mathbf{V} \subseteq \mathrm{Pol}\,\mathbf{M}$, since the basic operations of $\mathbf{V}$ are polynomials of $\mathbf{M}$. To prove the other inclusion, choose arbitrary $h \in \mathrm{Pol}_n \mathbf{M}$. By Claim 5 we get that

$$h(x_0, \ldots, x_{n-1}) = \sum_{i=0}^{n-1} \alpha_i \cdot x_i + c$$

where $\alpha_i(x) = h_i(x) - h_i(0) \in F$ and $c = h(0, \ldots, 0) \in M$. We have proved that $h \in \mathrm{Pol}\,\mathbf{V}$. We conclude that $\mathrm{Pol}\,\mathbf{V} = \mathrm{Pol}\,\mathbf{M}$ and the proof is finished. □

It remains to investigate two-element minimal algebras. Let us define the following operations on the set $\{0,1\}$: $\neg\, x = 1 - x$ (*negation*), $x \vee y = \max\{x,y\}$ (*join*), $x \wedge y = \min\{x,y\}$ (*meet*) and $x + y = (x+y) \bmod 2$ (*binary addition*).

3.12 Definition. We define the following seven algebras on the set $\{0,1\}$:

$$\mathbf{E}_0 = \langle\{0,1\}\rangle, \qquad \mathbf{E}_1 = \langle\{0,1\}, \neg\,\rangle, \qquad \mathbf{E}_2 = \langle\{0,1\}, +\rangle,$$
$$\mathbf{E}_3 = \langle\{0,1\}, \vee, \wedge, \neg\,\rangle, \qquad \mathbf{E}_4 = \langle\{0,1\}, \vee, \wedge\rangle,$$
$$\mathbf{E}_5 = \langle\{0,1\}, \vee\rangle, \qquad \mathbf{E}_6 = \langle\{0,1\}, \wedge\rangle.$$

3.13 Excercise. Every operation on $\{0,1\}$ is a polynomial of the two-element Boolean algebra $\mathbf{E}_3$.

Proof. Let $n > 0$ be arbitrary. We can regard n-ary operations on $\{0,1\}$ as characteristic functions of subsets of $\{0,1\}^n$. For any $f : \{0,1\}^n \to \{0,1\}$ we define the set $S_f \subseteq \{0,1\}^n$ as follows:

$$S_f \stackrel{\text{def}}{=} \{\bar{a} \in \{0,1\}^n \,:\, f(\bar{a}) = 1\}.$$

It is easy to see that $S_{f\wedge g} = S_f \cap S_g$, $S_{f\vee g} = S_f \cup S_g$ and $S_{\neg f} = {S_f}^C$ (where ^{C} denotes the complement in $\{0,1\}^n$). Let us denote

$$\mathcal{A} = \{A \subseteq \{0,1\}^n \,:\, \exists f \in \mathrm{Pol}_n\, \mathbf{E}_3 \text{ such that } A = S_f\}.$$

We want to prove that $\mathcal{A} = \mathcal{P}(\{0,1\}^n)$. We have that $\emptyset \in \mathcal{A}$, since the corresponding characteristic function is constant (and thus in $\mathrm{Pol}_n\, \mathbf{E}_3$). Let $\bar{a} = (a_0, \ldots, a_{n-1}) \in \{0,1\}^n$ be arbitrary. For each $0 \leq i < n$ we put

$$h_i(x) = \begin{cases} x & \text{if } a_i = 1, \\ \neg\, x & \text{if } a_i = 0. \end{cases}$$

Now, let us define the function $f_a \in \mathrm{Pol}_n\, \mathbf{E}_3$ in the following way:

$$f_a(x_0, \ldots, x_{n-1}) = \bigwedge_{i=0}^{n-1} h_i(x_i)$$

We see that $S_{f_a} = \{a\}$. For an arbitrary nonempty $A \subseteq \{0,1\}^n$ we define the n-ary polynomial

$$f = \bigvee_{a \in A} f_a.$$

We see that $S_f = \bigcup_{a\in A} S_{f_a} = \bigcup_{a\in A}\{a\} = A$. Thus we conlude that $\mathcal{A} = \mathcal{P}(\{0,1\}^n)$; and so every operation on $\{0,1\}$ is in $\mathrm{Pol}\, \mathbf{E}_3$. □

3.14 Definition. Let A be any set, $\preceq$ a partial order on A and $f : A^n \to A$ for some $n > 0$. We say that f **preserves the order** $\preceq$ iff $f(x_0, \ldots, x_{n-1}) \preceq f(x'_0, \ldots, x'_{n-1})$ whenever $x_i \preceq x'_i$ for all $0 \leq i < n$. Equivalently, the relation $\preceq$ is a subalgebra of $\mathbf{A}^2$, where $\mathbf{A} = \langle A, f \rangle$. We say that f **preserves order** if $\preceq$ is understood from the context.

3.15 Excercise. $\operatorname{Pol} \mathbf{E}_4$ is the set of all order preserving operations on $\{0, 1\}$ (we mean the usual order $0 \leq 1$).

Proof. It is easy to see that the composition of order preserving operations also preserves order. Since the projections and constant operations preserve order, we get that all $f \in \operatorname{Pol} \mathbf{E}_4$ preserve order.

To prove the other inclusion, let $f = f(x_0, \ldots, x_{n-1})$ be an arbitrary order preserving n-ary operation on $\{0, 1\}$. For any $\bar{a} \in \{0, 1\}^n$ let us set

$$g_{\bar{a}}(x_0, \ldots, x_{n-1}) = \bigwedge_{0 \leq i < n,\, a_i = 1} x_i$$

and then

$$f' = \bigvee_{\bar{a} \in \{0,1\}^n,\, f(\bar{a}) = 1} g_{\bar{a}}$$

(it is understood that $\bigwedge \emptyset = 1$ and $\bigvee \emptyset = 0$).

We shall prove that $f = f'$. Choose arbitrary $\bar{c} \in \{0, 1\}^n$. If $f(\bar{c}) = 1$, then $f'(\bar{c}) \geq g_{\bar{c}}(\bar{c}) = 1$. Let $f(\bar{c}) = 0$ and suppose for contradiction that $f'(\bar{c}) = 1$. It follows that for some $\bar{a} \in \{0, 1\}^n$ with $f(\bar{a}) = 1$ we have $g_{\bar{a}}(\bar{c}) = 1$. But then $\{i : a_i = 1\} \subseteq \{i : c_i = 1\}$, and thus $a_i \leq c_i$ for all i. Since f preserves order, we have that $1 = f(\bar{a}) \leq f(\bar{c}) = 0$, a contradiction. We conclude that $f = f' \in \operatorname{Pol}_n \mathbf{E}_4$. □

3.16 Excercise. Let $\mathbf{A} = \langle A, \ldots \rangle$ be an algebra and $\preceq$ a partial order on A. If $\operatorname{Pol} \mathbf{A}$ is not contained in the set of operations on A that preserve $\preceq$, then there exists $f \in \operatorname{Pol}_1 \mathbf{A}$ which doesn't preserve $\preceq$.

Proof. Let $n > 0$ and $h \in \operatorname{Pol}_n \mathbf{A}$ be such that h doesn't preserve $\preceq$. There exist $\bar{a} = (a_0, \ldots, a_{n-1}), \bar{b} = (a_0, \ldots, a_{n-1}) \in A^n$ such that $a_i \preceq b_i$, $0 \leq i < n$ and $h(\bar{a}) \not\preceq h(\bar{b})$.

We define a finite sequence $(c_i)_{i=0}^n$ of elements of A as follows:

$$\begin{aligned} c_i &= h(a_0, a_1, \ldots, a_{i-1}, b_i, b_{i+1}, \ldots, b_{n-1}),\ 0 \leq i < n, \\ c_n &= h(a_0, \ldots, a_{n-1}). \end{aligned}$$

Since $c_0 = h(\bar{b}) \not\succeq h(\bar{a}) = c_n$, it follows by the transitivity of $\preceq$ that for some j, $0 \leq j < n$ we have $c_j \not\succeq c_{j+1}$. We define the unary polynomial f as follows:

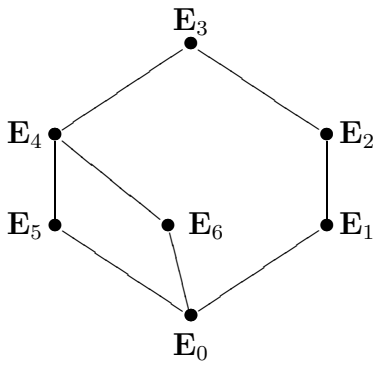
$$f(x) = h(a_0, a_1, \ldots, a_{j-1}, x, b_{j+1}, \ldots, b_{n-1}).$$

Now $a_j \preceq b_j$, but $f(a_j) = c_{j+1} \not\preceq c_j = f(b_j)$; and so f doesn't preserve $\preceq$. □

Notice that $\neg$ is the only unary operation on $\{0,1\}$ that doesn't preserve order. Thus it follows from the previous two excercises that for any $\mathbf{A} = \langle \{0,1\}, \ldots \rangle$, if $\operatorname{Pol} \mathbf{A} \not\subseteq \operatorname{Pol} \mathbf{E}_4$ then $\neg \in \operatorname{Pol}_1 \mathbf{A}$.

3.17 Theorem. *Every algebra $\mathbf{M} = \langle \{0,1\}, \ldots \rangle$ is polynomially equivalent to one of the algebras $\mathbf{E}_0, \ldots, \mathbf{E}_6$, no two of which are polynomially equivalent.*

The algebras $\mathbf{E}_0, \ldots, \mathbf{E}_6$ ordered by the inclusion among their polynomial clones form a lattice pictured below.



Proof. First, suppose that all polynomial operations of $\mathbf{M}$ depend on at most one variable. Since $\operatorname{Sym}\{0,1\}$ has only the trivial subgroups, by Lemma 3.10 it follows that $\mathbf{M}$ is polynomially equivalent to $\mathbf{E}_0$ or $\mathbf{E}_1$.

If $\mathbf{M}$ has a polynomial operation depending on at least two variables, then by Lemma 3.2 it has at least one binary polynomial operation that depends on both its variables. Let us denote

$$\mathrm{D} \stackrel{\text{def}}{=} \{f \in \operatorname{Pol}_2 \mathbf{M} : f \text{ depends on both variables}\} \neq \emptyset.$$

Notice that the multiplication table of any $f \in \mathrm{D}$ has a non-constant row and a non-constant column. There are only 10 such binary operations on the set $\{0,1\}$. Two of them preserve order, the join and the meet:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

Next, there are two operations with all columns and rows non-constant, the binary addition $+$ and the operation $\beta = x + y + 1$:

$+$	0	1
0	0	1
1	1	0

β	0	1
0	1	0
1	0	1

The remaining six operations are γ_i, $1 \leq i \leq 6$ (see the multiplication tables below). Let us denote $\mathrm{K} = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_4, \gamma_6\}$.

γ_1	0	1
0	0	1
1	0	0

γ_2	0	1
0	1	0
1	0	0

γ_3	0	1
0	0	0
1	1	0

γ_4	0	1
0	1	0
1	1	1

γ_5	0	1
0	1	1
1	1	0

γ_6	0	1
0	1	1
1	0	1

It is important to notice that if we have $\neg \in \operatorname{Pol}\mathbf{M}$, then for any $f = f(x, y) \in \operatorname{Pol}_2\mathbf{M}$ the operations $f(\neg x, y)$, $f(x, \neg y)$ and $\neg f(x, y)$ are also in $\operatorname{Pol}_2\mathbf{M}$. Thus we can switch the rows and columns of the multiplication table of f and also invert its entries (i.e., put 1's instead of 0's and vice versa) and the resulting operation is still a polynomial of $\mathbf{M}$. We will divide the rest of the proof into three cases.

Case 1. Assume that $\mathrm{D} \cap \mathrm{K} \neq \emptyset$.

Since each $\gamma_i \in \mathrm{K}$ has $(1, 0)$ as a row or a column, by substituting one of the variables with 0 or 1 we get that $\neg \in \operatorname{Pol}\mathbf{M}$. (It also follows from Excercise 3.16, since none of the γ_i's preserves order). Therefore it is not hard to see that $\vee, \wedge \in \operatorname{Pol}\mathbf{M}$. It now follows from Excercise 3.13 that in this case $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_3$.

Case 2. Let $\mathrm{D} \cap \mathrm{K} = \emptyset$ and $\mathrm{D} \cap \{\vee, \wedge\} \neq \emptyset$.

Assume that $\wedge \in \mathrm{D}$ (if $\vee \in \mathrm{D}$, then the proof is very similar). If $\mathbf{M}$ has a polynomial operation that doesn't preserve order, then $\neg \in \operatorname{Pol}\mathbf{M}$ (see Excercise 3.16); and thus also $\vee \in \operatorname{Pol}_2\mathbf{M}$. We conclude that $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_3$.

Now suppose that all polynomials of $\mathbf{M}$ preserve order. From Excercise 3.15 we get that $\operatorname{Pol}\mathbf{M} \subseteq \operatorname{Pol}\mathbf{E}_4$. We will prove that if $\operatorname{Pol}\mathbf{E}_6 \subsetneqq \operatorname{Pol}\mathbf{M}$, then $\vee \in \operatorname{Pol}\mathbf{M}$; and so $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_4$.

Let h be an n-ary polynomial such that $h \notin \operatorname{Pol}\mathbf{E}_6$. For any subset $I \subseteq \{0,\ldots,n-1\}$ we define $\bar{x}_I = (x_0,\ldots,x_{n-1}) \in \{0,1\}^n$ with $x_i = 1$ iff $i \in I$ ($\bar{x}_I$ is the characteristic function of I). Since we are now assuming that all polynomials of $\mathbf{M}$ preserve order, it follows that $h(\bar{x}_I) \leq h(\bar{x}_J)$ whenever $I \subseteq J$. Let us define

$$\mathcal{I} \stackrel{\text{def}}{=} \{I \subseteq \{0,\ldots,n-1\} \,:\, h(\bar{x}_I) = 1\}.$$

Since h is not constantly equal to 0, $\mathcal{I}$ is nonempty. We will prove that $\mathcal{I}$ has at least two minimal members I_0, I_1. Suppose for contradiction that I_0 is the only minimal member of $\mathcal{I}$. Then $h(\bar{x}_I) = 1$ iff $I_0 \subseteq I$. It follows that

$$h(x_0,\ldots,x_{n-1}) = \bigwedge_{i\in I_0} x_i,$$

a contradiction with $h \notin \operatorname{Pol}\mathbf{E}_6$. Let us now consider the binary operation $b \in \operatorname{Pol}\mathbf{M}$ defined with

$$b(x,y) = h(g_0(x,y), g_1(x,y), \ldots, g_{n-1}(x,y)),$$

where the binary operations g_i $(0 \leq i < n)$ are defined as follows:

$$g_i(x,y) = \begin{cases} x & \text{if } i \in I_0 - I_1, \\ y & \text{if } i \in I_1 - I_0, \\ 1 & \text{if } i \in I_1 \cap I_0, \\ 0 & \text{if } i \notin I_1 \cup I_0. \end{cases}$$

We will prove that $b(x,y) = x \vee y$. We have that $b(1,0) = h(\bar{x}_{I_0}) = 1$, $b(0,1) = h(\bar{x}_{I_1}) = 1$. Since $I_0 \cup I_1 \supseteq I_0$, it follows that $b(1,1) = h(\bar{x}_{I_0\cup I_1}) = 1$. Finally, $b(0,0) = h(\bar{x}_{I_0\cap I_1}) = 0$ follows from the fact that $I_0 \cap I_1 \subsetneqq I_0$ and I_0 is a minimal member of $\mathcal{I}$. We have proved that $\vee \in \operatorname{Pol}\mathbf{M}$; and so $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_4$.

Case 3. Assume that $\mathrm{D} \subseteq \{+, \beta\}$.

Since $\neg \in \operatorname{Pol}\mathbf{M}$ and $+ = \neg\, \beta$, we have that $+ \in \mathrm{D}$. We will prove that $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_2$. An n-ary operation f on $\{0,1\}$ is called *affine* iff $f(x_0,\ldots,x_{n-1}) = \sum_{i=0}^{n-1} a_i x_i + c$ for some $n > 0$ and $a_i, c \in \{0,1\}$. Since the

projections and constant operations are affine and the composition of affine operations is affine, we see that $\operatorname{Pol}\mathbf{E}_2$ is the set of all affine operations on $\{0,1\}$.

Suppose for contradiction that $\operatorname{Pol}\mathbf{M}$ has an operation which is not affine and let $h : \{0,1\}^n \to \{0,1\}$ be such an operation with minimal arity. Notice that all unary operations on $\{0,1\}$ are affine.

First, we will prove by the way of contradiction that h is binary. Let $n > 2$. We define $c = h(0,0,0\ldots,0)$ and $a_i = h(0,\ldots,0,1,0,\ldots,0) - c$ for each $0 \leq i < n$ (the '1' occuring in the i-th place). The $(n-1)$-ary function $h(0,x_1,\ldots,x_{n-1})$ is affine and it is easily seen that

$$h(0,x_1,x_2,x_3\ldots,x_{n-1}) = a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_{n-1}x_{n-1} + c.$$

Similarly, we get that

$$\begin{aligned}
h(x_0,0,x_2,x_3\ldots,x_{n-1}) &= a_0x_0 + a_2x_2 + a_3x_3 + \cdots + a_{n-1}x_{n-1} + c,\\
h(x_0,x_1,0,x_3\ldots,x_{n-1}) &= a_0x_0 + a_1x_1 + a_3x_3 + \cdots + a_{n-1}x_{n-1} + c.\\
&\vdots\\
h(x_0,x_1,x_2,\ldots,x_{n-2},0) &= a_0x_0 + a_1x_1 + a_2x_2 + \cdots + a_{n-2}x_{n-2} + c.
\end{aligned}$$

If we define an affine operation $h'(x_0,\ldots,x_{n-1}) = \sum_{i=0}^{n-1} a_ix_i + c$, we get that $h'(\bar{x}) = h(\bar{x})$ for all $\bar{x} \neq (1,1,\ldots,1)$. Now, the operation $h(1,x_1,\ldots,x_{n-1})$ is also affine and

$$\begin{aligned}
h(1,0,0,\ldots,0) &= h'(1,0,0,\ldots,0) = a_0 + c,\\
h(1,1,0,\ldots,0) &= a_0 + a_1,\\
&\vdots\\
h(1,0,0,\ldots,1) &= a_0 + a_n.
\end{aligned}$$

It follows that $h(1,x_1,x_2,\ldots,x_{n-1}) = a_0 + \sum_{i=1}^{n-1} a_ix_i + c$; and consequently $h(1,1,\ldots,1) = h'(1,1,\ldots,1)$. We conclude that $h = h'$ is affine, which is a contradiction.

We have proved that if $\operatorname{Pol}\mathbf{M}$ has an operation which is not affine, then it has a binary non-affine operation. Since all binary operations depending on less than two variables are affine, such an operation has to depend on both its variables, which is in contradiction with $\mathrm{D} \subseteq \{+,\beta\}$ (both $+$ and β are affine). Thus we have proved that $\operatorname{Pol}\mathbf{M} = \operatorname{Pol}\mathbf{E}_2$.

To finish the proof of this theorem, it remains to show that the algebras $\mathbf{E}_0, \ldots, \mathbf{E}_6$ are polynomially inequivalent (i.e., their polynomial clones are pairwise different). In the above we have proved that for each $n > 0$, $\mathrm{Pol}_n \mathbf{E}_3$ is the set of all n-ary operations on $\{0, 1\}$, $\mathrm{Pol}_n \mathbf{E}_4$ are the order preserving operations and $\mathrm{Pol}_n \mathbf{E}_2$ are the affine ones. From the above proof (Case 2) we can also conclude that $\mathrm{Pol}\,\mathbf{E}_5 \neq \mathrm{Pol}\,\mathbf{E}_6$ and $\mathrm{Pol}\,\mathbf{E}_5, \mathrm{Pol}\,\mathbf{E}_6 \subsetneqq \mathrm{Pol}\,\mathbf{E}_4$. Since $\mathbf{E}_0$ and $\mathbf{E}_1$ don't have any polynomial operations depending on two variables, we conclude that all the polynomial clones $\mathrm{Pol}\,\mathbf{E}_0, \ldots, \mathrm{Pol}\,\mathbf{E}_6$ are pairwise different (the rest of the inclusions is obvious); and the proof is finished. □

The algebras $\mathbf{E}_5$ and $\mathbf{E}_6$ are isomorphic. Any algebra isomorphic to one of them is called a *two-element semilattice*. An algebra is called a *two-element lattice* iff it is isomorphic to $\mathbf{E}_4$ and a *two-element Boolean algebra* iff it is isomorphic to $\mathbf{E}_3$.

3.18 Definition. Let $\mathbf{M}$ be a minimal algebra.

(1) $\mathbf{M}$ is of **type 1** (**unary type**), iff $\mathrm{Pol}\,\mathbf{M} = \mathrm{Pol}\,\langle M, \Pi\rangle$ for a subgroup $\Pi \leq \mathrm{Sym}\, M$.

(2) $\mathbf{M}$ is of **type 2** (**affine type**), iff $\mathbf{M}$ is polynomially equivalent to a vector space.

(3) $\mathbf{M}$ is of **type 3** (**Boolean type**), iff $\mathbf{M}$ is polynomially equivalent to a two-element Boolean algebra.

(4) $\mathbf{M}$ is of **type 4** (**lattice type**), iff $\mathbf{M}$ is polynomially equivalent to a two-element lattice.

(5) $\mathbf{M}$ is of **type 5** (**semilattice type**), iff $\mathbf{M}$ is polynomially equivalent to a two-element semilattice.

3.19 Corollary. *A finite algebra is minimal iff it is of one of the types **1**-**5**.*

Proof. This is an immediate consequence of Lemma 3.10, Theorem 3.11 and Theorem 3.17. □

Let $\mathbf{A}$ be a finite algebra and $\alpha \prec \beta$ a prime quotient in $\mathrm{Con}\,\mathbf{A}$. Let U be an $\langle\alpha, \beta\rangle$-minimal set and $N \subseteq U$ an $\langle\alpha, \beta\rangle$-trace. From Lemma 2.17 it follows that we can assign one of the types **1**-**5** to N.

Moreover, in chapter 4 of the book [3] it is proved that all traces of $\mathbf{A}|_U$ posses the same type and since all $\langle \alpha, \beta \rangle$-minimal sets have the same set of traces (up to isomorphism), we can assign one of the types **1**-**5** to the prime quotient $\alpha \prec \beta$.

In this way, we can consider the congruence lattice of $\mathbf{A}$ as a labeled graph, where all of the prime quotients are labeled with one of the five types defined above.

Bibliography

[1] Bulatov A. A., Krokhin A. A., Jeavons P.: *Constraint Satisfaction Problems And Finite Algebras*. Proceedings of the 27th International Colloquium on Automata, Languages and Programming, 272–282, 2000.

[2] Clark D. M., Davey B. A.: *Natural Dualities for the Working Algebraist*. Cambridge University Press, 1998.

[3] Hobby D., McKenzie R.: *The Structure of Finite Algebras*. Contemp. Math., vol. 76, Amer. Math. Soc. (Providence, R.I.), 1988.

[4] Idziak P. M.: *A characterization of finitely decidable congruence modular varieties*. Transactions of the American Mathematical Society, Vol. 349, No. 3 (1997) 903–934.

[5] McKenzie R., Valeriote M.: *The Structure of Decidable Locally Finite Varieties*. Birkhauser, Progress in Mathematics, Volume 79 (1989).